Thesis: Navigation in GNSS denied environments using software defined radios and LTE signals of opportunities

Nazir Ikhtiari

A thesis submitted in partial fulfilment
of the requirements for the degree of
Master of Engineering
in
Electrical and Computer Engineering
at the
University of Canterbury,
Christchurch, New Zealand.

19 May 2019

ABSTRACT

The aim of this project is to implement a positioning system based on existing technologies as a backup for GNSS to be used in an Unpiloted Aerial Vehicle (UAV) designed for carrying passengers where a backup is a necessity. The project sponsors have set a target accuracy of <100 m.

A comprehensive list of existing and potential positioning technologies were assessed and LTE was selected as the most suitable, mainly based on accuracy, coverage, and availability. Other factors such as size, weight, power, and cost were also considered. LTE is a 4^{th} generation cellular technology, used worldwide, and likely to be around for another decade. It presents the best accuracy based on current literature with [37] claiming GPS level accuracy.

LTE has two methods of positioning that do not require any changes to the network, 1) using Timing Advance (TA) and, 2) using LTE Signals Of Opportunities (SOP). Both were assessed; first the TA method, then the SOP method.

The TA value is a measure of the round trip time of the LTE signal from a Mobile Station (MS) to the Base Station (BS) and back. It has a granularity of 78 m, and hence, a theoretical positioning accuracy of 78 m. A Ublox cellular module was used to assess the suitability of TA for positioning. A practical accuracy of 300 m (95 % probability) with an update rate of 20 s per update was achieved. This result does not meet the accuracy criteria and its update rate of 18 s/update is lower than desired.

The SOP method tracks the Time-Of-Arrival (TOA) of LTE pilot sequences (i.e., signals of opportunities) and uses them to get the distance between the MS and BS. By getting distances to four BSs, the MS can uniquely identify its position. The pilot sequences were tracked using a LTE software defined radio made up of a USRP B200mini radio front-end and srsUE (an open source software implementation of an LTE MS written in C and C++). The resolution of the TOAs is one sampling period (T_s); which at 23.04 MHz equates to a positioning granularity and theoretical accuracy of 13 m.

In practice, the TOAs were detected to a resolution of 130–254 ns (95 % probability) depending on the environment. Both results were obtained from tests carried out at ground level where multipath was present. This result leads to a practical accuracy of 39–76 m (95 % probability) respectively, although this does not take into account time

drift. To detect TOAs with sub T_s resolution, the Blais-Rioux peak detector algorithm [15] can be used. A possible method of removing multipath is provided in [24].

The biggest source of error in the system was the MS clock's time drift (i.e., its time drifting away from real time). Hence, a practical and reliable positioning system will have to use a higher quality clock and/or a robust method of modelling and compensating its drift. This is difficult with low quality clocks such as the B200mini's Temperature Compensated Crystal Oscillator (TCXO), whose drift was found to be non-linear and volatile; changing from trial to trial. Hence a higher quality clock is recommended, since its drift rate is smaller and also linear over a much longer time, making it easier to model and compensate.

A list of even higher quality clocks (for the MS and BS) are also provided, which would enable the time drift of the overall system to be negligible for the entire flight of the UAV, i.e., for ∼60 minutes after GNSS signal loss. Upgrading BS clocks is likely infeasible. The Spark networks current BSs are equipped with high precision Oven Controlled Crystal Oscillator (OCXO) [42] and disciplined by GPS; which means that their drift is constantly corrected, and cannot be observed and modelled for drift compensation. Without drift compensation a BS clocks time drift will likely exceed an error of 100 m in 5–10 minutes, which may only be suitable for emergency landings.

Overall, the LTE SOP method provides satisfactory positioning results, but a fully implemented practical and reliable system will need more research and development and system components are likely to be relatively expensive.

CONTENTS

ACKNOWLEDGEMENTS

I would like to thank my supervisors Adriel Kind and Michael Hayes for their technical support and guidance throughout this project.

Thank you also to my industry mentors, Zouhair Mahboubi and Herve Martins Rivas, for organising this project through which I have gained a significant amount of valuable knowledge and experience. Thank you also for your guidance and technical support.

Thank you Geoff Tunnicliffe and Andrew Leckie from Spark for providing me information that was difficult to obtain or not available publicly.

Thank you also to all the other people at the Wireless Research Centre and at the University of Canterbury who helped me with this project. Thank you for your valuable discussions and for making this project worthwhile.

ABBREVIATIONS AND ACRONYMS

ACK	ACKnowledgement (in ARQ protocols)
ADF	Automatic Direction Finder
AGL	Above Ground Level
BCCH	Broadcast Control CHannel
BCH	Broadcast CHannel
BS	Base Station
CCCH	Common Control CHannel
CDMA	Code Division for Multiple Access
CID	Cell ID
COTS	Commercially Available Off the Shelf
CP	Cyclic Prefix
C-RNTI	Cell Radio-Network Temporary Identifier
CRS	Cell-specific Reference Signal
CS	Circuit Switched
CSAC	Chip Scale Atomic Clock
DCCH	Dedicated Control CHannel
DCI	Downlink Control Information
DL	Downlink
DL-SCH	Downlink Shared CHannel
DME	Distance Measuring Equipment
eNB	E-UTRAN NodeB (an LTE BS is known as an eNB)
FDD	Frequency Division Duplex
GNSS	Global Navigation Satellite System
GPSDO	GPS Disciplined Oscillator
HARQ	Hybrid Automatic Repeat reQuest

LCID	Logical CHannel Index
LMU	Location Measurement Unit
LOS	Line Of Sight
MAC	Medium Access Control
MCCH	MBMS Control CHannel
MCH	Multicast CHannel
MS	Mobile Station (a.k.a terminal or user equipment)
NAK, NACK	Negative ACKnowledgement (in ARQ protocols)
NDB	Non-Directional Beacon
PBCH	Physical Broadcast CHannel
PCCH	Paging Control CHannel
PCFICH	Physical Control Format Indicator CHannel
PCH	Paging CHannel
PCI	Physical Cell ID
PDCCH	Physical Downlink Control CHannel
PDN	Packet Data Network
PDSCH	Physical Downlink Shared CHannel
PDU	Protocol Data Unit
PHICH	Physical Hybrid-ARQ Indicator CHannel
PHY	Physical Layer
PMCH	Physical Multicast CHannel
PRACH	Physical Random Access CHannel
P-RNTI	Paging RNTI
PRS	Positioning Reference Signal
PS	Packet Switched
PSS	Primary Synchronisation Signal
PSTN	Public Switched Telephone (Mobile) Network
PUCCH	Physical Uplink Control CHannel
PUSCH	Physical Uplink Shared CHannel
RACH	Random Access CHannel
RAN	Radio Access Network
RAR	Random Access Response
RA-RNTI	Random Access RNTI
RAT	Radio Access Technology
RB	Resource Block

RE	Resource Element
RLC	Radio Link Control
RNC	Radio Network Controller
RNTI	Radio-Network Temporary Identifier
RRC	Radio Resource Controller
RTT	Round Trip Time
SDR	Software Define Radio
SDU	Service Data Unit
SIB	System Information Block
SI-RNTI	System Information RNTI
SNR	Signal to Noise Ratio
SOP	Signals Of Opportunity
SRS	Sounding Reference Signal
SSS	Secondary Synchronization Signal
SSV	Standard Service Volume
TDD	Time Division Duplex
TOA	Time Of Arrival
UAV	Unpiloted Aerial Vehicle
UCI	Uplink Control Information
UL	Uplink
UE	User Equipment (the 3GPP name for mobile terminal or mobile station)
UL-SCH	Uplink Shared CHannel
UTRA	Universal Terrestrial Radio Access
UTRAN	UTRA Network
VOR	VHF Omnidirectional Range
XO	Xtal (Crystal) Oscillator

Chapter 1

INTRODUCTION

Many applications nowadays require positioning. It is for this reason that more and more devices, e.g. mobile phones, personal vehicles, drones, trucks, aeroplanes, etc. are being embedded with devices that provide positioning capabilities. Although Global Navigation Satellite Systems (GNSS) require a huge initial investment that requires numerous satellites to be placed in orbit around the earth, once implemented, GNSS systems provide by far the cheapest form of positioning. It is for this reason that GNSS is available in almost all devices with positioning capabilities.

GNSS, in particular GPS, having 31 satellites already orbiting the earth is the most widely available positioning method available. GNSS also provides the most accurate positioning, capable of centimetre level accuracy in expensive receivers under open-sky conditions. But GPS isn't always reliable or available. GNSS does not work underground and in multistory buildings as the weak signals are unable to penetrate through multiple or thick walls/roofs to reach those GNSS receivers. It is also prone to jamming and spoofing (a technique where imitated GNSS signals send false GNSS coordinates to GNSS receivers, making the receiver believe it is in a particular location when it is actually somewhere else). In large cities with large building, GNSS is not reliable even outdoor, as a result of multipath errors caused due to reflections of GNSS signals off structures; these can cause positioning errors of several hundred metres. In the urban canyons of large cities large structures may get in the way of GNSS signals such that the GNSS receiver is unable to get signals from at least 4 satellites to provide a unique position fix.

It is for these reasons that there is still a lot of ongoing research in to other positioning methods, and also why old terrestrial based positioning methods used for aviation, e.g. VHF Omnidirectional Range (VOR), Distance Measuring Equipment (DME), Non-Directional Beacons (NDB), LOng RAnge Navigation (LORAN), etc., are still being kept as a backup.

Currently aeroplanes use primarily GNSS for navigation, but there are several other backups as mentioned before such as VOR, DME, and NDB, that are used to provide coarse positioning when GNSS is not available. Instrument landing systems (ILS) and

locator beacons provide accurate positioning during landing. These aeroplanes also have highly trained pilots capable of navigating visually when no positioning technologies are available.

An Unpiloted Aerial Vehicle (UAV), designed to fly within or around cities, must be able to navigate in those areas safely without a pilot. Although it is likely to be flying above buildings for the majority of its flight, where the UAV will be in Line-Of-Sight (LOS) of GNSS signals and there is no multipath, multipath will be an issue during landing. There is also the issue due to jamming and spoofing. Hence, it is very important for UAVs to have a backup positioning systems that can provide relatively accurate positioning at all times when GNSS cannot be relied on.

1.1 MOTIVATION

Most vehicles, regardless of whether they operate on the ground or in the air, use GNSS for positioning. The most widely used is GPS (the GNSS constellation owned by the US government). But GNSS is not always reliable. Hence, for an UAV that is designed to carry passengers having a reliable positioning system at all times is mandatory in order to get certified for flying passengers. Is is for this reason, that a backup positioning system is required.

1.2 OBJECTIVES

The purpose of this project is to improve the autonomous positioning capabilities of an industry partner by investigating alternative navigation solutions, i.e., researching a suitable positioning technology to be used as a backup for GNSS denied scenarios, that can be combined with dead-reckoning. These capabilities will eventually be integrated and tested on the full-scale platform in follow up projects.

The technologies to be researched include VOR, DME, NDB, cellular positioning, etc.. A prototype would then be built to test and evaluate the backup systems characteristics. The prototype might be flown on board a piloted General Aviation (GA) aircraft in order to collect representative data. The majority of the testing will be carried out at the University of Canterbury's Spatial Engineering Research Centre (SERC), using ground based emulation.

1.3 THESIS OUTLINE

The structure of this thesis is the following:

Chapter 1 introduces the project as well detailing the motivation and objectives of the project.

A list of existing and potential positioning technologies are described in chapter 2, which will discuss how each positioning technology works, and also show their accuracy, coverage, availability, power, cost, and weight. At the end of this chapter a trade-off analysis is used to select the most suitable positioning technology, which is further explored in subsequent chapters.

The most suitable positioning technology, in this case LTE (chosen from chapter 2), is further explored in chapters 3 and 4. Each chapter tests a different LTE positioning method.

An LTE positioning method based on Timing Advance (TA) is tested in Chapter 3. The chapter begins by explaining what TA is, how it can be used for positioning, and the hardware and software required to get it working. It then presents the system's positioning results, followed by conclusions and future work.

In chapter 4, a positioning system based on LTE pilot sequences (i.e., signals of opportunities) is discussed. The chapter begins by introducing the pilot sequences, explaining how they can be used for positioning, and the hardware and software required to get it working. Following this, the experiment and positioning results are presented, followed by various ways of improving/achieving a feasible position system. The chapter finishes by providing conclusions and outlining the future work. The end of this chapter marks the end of the thesis.

Chapter 2

POTENTIAL BACKUPS FOR GNSS

The purpose of this chapter is to look at various positioning systems that are currently used in aviation that can be used as a backup for GNSS. Following that, other radio signals known as Signals Of Opportunities (SOP[1]) will be explored that could potentially be used for positioning. At the end of this chapter, a trade-off analysis will be used to compare the list of technologies researched, and the most suitable technology will be further researched and implemented as a backup for GNSS.

[1]They are known as SOPs because they are not designed for positioning but are opportunistically being used for positioning. Cellular signals are one example.

2.1 NON-DIRECTIONAL BEACON (NDB) AND ASSOCIATED AUTOMATIC DIRECTION FINDER (ADF)

2.1.1 Non-Directional Beacon (NDB)

A Non-Directional Beacon is an aviation and marine navigational aid. The ground beacon, situated at a known location, transmits an omnidirectional radio signal which is modulated at intervals with the identification code [13]. The associated Automatic Direction Finder (ADF), situated on an aircraft, senses this signal and is able to determine the direction of the NDB beacon. NDBs normally operate in the 190–535 kHz frequency band, although ICAO Annex 10 specifies a frequency range from 190–1750 kHz. They are identified by a one, two, or three letter, Morse code call-sign. The ID code is a 400 or 1020 Hz tone superimposed on the carrier [3].

There are four types of NDBs used in aviation:

- En route NDBs, used to mark airways.
- Approach NDBs: where two NDBs are sited to provide an instrument approach to landing [13].
- Localizer beacons.
- Locator beacons.

The last two types are used with Instrument Landing Systems (ILS) and are also known as compass locators [46]. Compass locators are NDBs usually co-located with the outer marker (OM) and middle marker (MM) beacons; see Figure 2.1. They have a power of less than 25 W, a range of at least 15 NM, and operate in the 190–535 kHz frequency band.

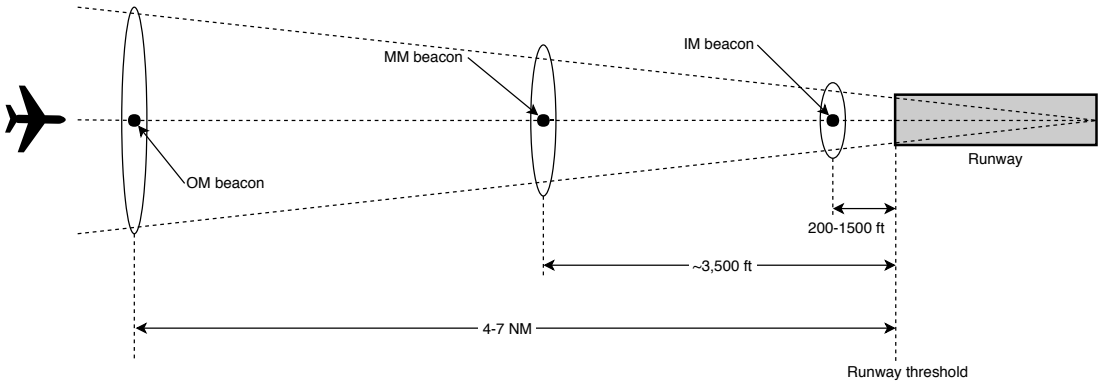


Figure 2.1 Outer marker, middle marker, and inner marker (IM) locations relative to a runway. The OM, MM, and IM beacons are normally located 4-7 NM, ∼3,500 ft, and 200–1500 ft, respectively, from the runway threshold on the extended centre line of the runway [3].

Most NDBs are installed in pairs (i.e., main, and standby). If certain monitored parameters are out of tolerance, the standby is activated [13]. These parameters include:

- Excessive hum.
- Reduction of carrier power.
- Failure or reduction in level of ID code.

2.1.2 Automatic Direction Finder (ADF)

The ADF has two antennas. A directional loop antenna that is physically rotated (in old systems) so that it aligns with the radio signal for maximum signal strength, or rotated 90° clockwise or counterclockwise to detect a signal null. In practice, it is the null position that is used as it can be much more accurately detected.

The loop antenna gives two signal nulls 180° apart, indicating that the NDB station is in one of two possible directions, 180° apart. To determine which one, the signal from a non-directional fixed antenna, called a "sense" antenna is mixed with signals from the loop antenna and combines in a way that orientates the loop antenna in the correction direction [12]. The compass pointer on the ADF monitor, is offset by plus or minus 90° to account for this offset [13].

On modern ADFs, the loop antenna does not move but instead uses multiple fixed antennas that are electronically commutated [18]. Figure 2.2 shows the block diagram of an aircraft ADF system using a mechanically rotatable antenna. Figure 2.3 shows a modern ADF antenna with no moving parts.

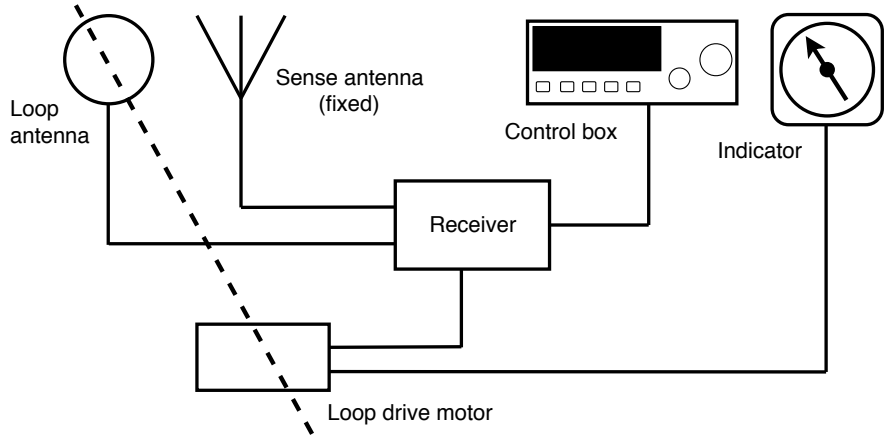


Figure 2.2 ADF system block diagram using a mechanically rotatable loop antenna [13].

2.1.2.1 Airborne Equipment

The loop antenna is a flat loop usually located on the belly of the aircraft while the sense antenna is a long wire that runs from the top of the tail to the top of the cabin. On large aircraft the sense antenna may be located on the belly.

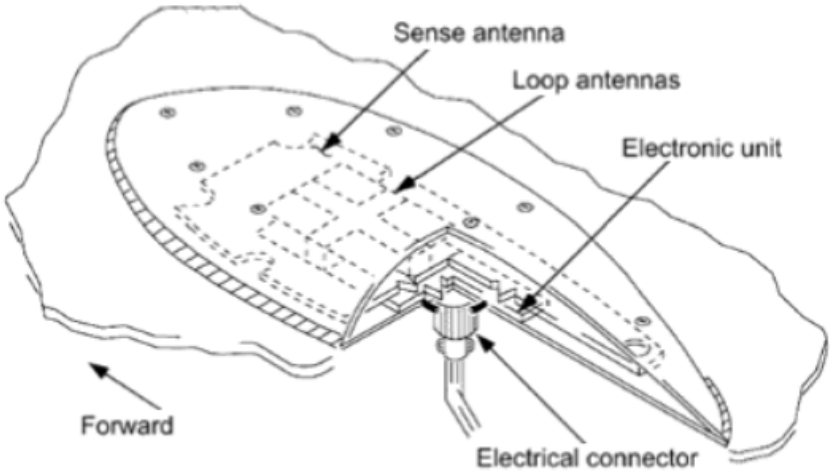


Figure 2.3 Modern ADF antenna with no moving parts [18].

More modern ADFs have a combined loop and sense antenna that is usually located on the belly of the aircraft. These work far better than the old antennas, cause less drag, and are less prone to icing [41]. See Figure 2.3.

2.1.2.2 Modes of Operation

The NDB channel is selected using the ADF control box by turning a knob. The control box is also used to select the mode of operation [41].

- **ANT mode:** The loop antenna is disabled and all receiving is done through the sense antenna. This provides the clearest audio reception and is typically used when identifying an NDB station.
- **ADF mode:** Both antennas are enabled and the ADF indicator points to the NDB station. Figure 2.4 shows a typical ADF indicator and control.

2.1.2.3 Limitations

- **Night effect:** Radio waves transmitted from an NDB take two paths. One path is along the surface of the earth, known as ground waves, and the other is up known as sky waves; see Figure 2.5. At night, especially around dusk or dawn when changes in the state of ionization in the ionosphere are particularly violent, the sky waves are reflected back and interfere with the ground waves. The ground waves alone would cause the ADF indicator to point directly to the NDB beacon, but as the sky waves are out-of-phase with the ground waves, it causes the ADF indicator to become erratic [13].

Figure 2.4 ADF indicator instrument and control box [3].

At night the range of an NDB is only reliable for distances up to 60 NM for land and 100 NM over water. Beyond this, the sky waves predominate over the ground waves causing the ADF indicator to become erratic [13].

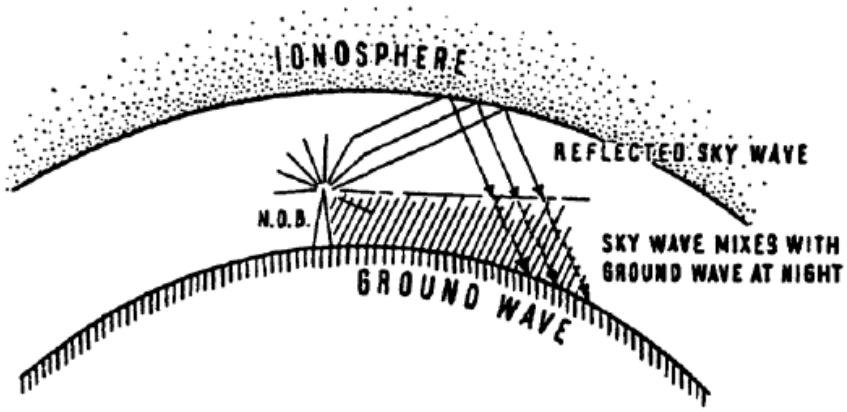


Figure 2.5 Reflected waves from the ionosphere interfering with ground waves [13].

- **Co-channel interference:** Interference can happen from other NDBs, e.g., signals from another NDB with the same channel frequency or signals from an NDB with an adjacent frequency received with high enough power.

  This is not usually a problem during the day, but at night, and in particular during dusk or dawn, when the range of sky waves increases considerably due to reflections, co-channel and adjacent channel interference can take place [13].

- **Mountain/Terrain effect:** The range of an NDB is also affected by terrain. The range is greatest over the sea and least over sandy and mountainous regions. An NDB with a daylight range of 600 NM over sea may only have a 100 NM

Class	**Distance (Radius)**
Compass Locator	15 NM
MH	25 NM
H	50 NM*
HH	75 NM
*Service ranges of individual facilities may be less than 50 nautical miles (NM). Restrictions to service volumes are first published as a Notice to Airmen and then with the alphabetical listing of the NAVAID in the Chart Supplement U.S.	

Table 2.1 NDB standard service volume [46].

range over rough terrain. Thus an NDB beacon located on a coastline can have significantly greater range towards the sea, then towards land [13].

Rough terrain like mountains and cliffs can cause reflections, producing a similar effect to night effect where there are two waves; a direct wave and a reflected out-of-phase wave [13].

- **Thunderstorm effect:** Thunderstorms can generate a significant amount of radio frequency energy. Hence, when near a thunderstorm the ADF pointer may point towards the storm rather than the NDB station. When in the vicinity of a thunderstorm bearing accuracy should be checked by other means [13].
- **Height effects:** The range of NDB across water is relatively independent of aircraft height but over unfavourable terrain the signal range increases considerably with height [13].

2.1.2.4 Characteristics

- **Standard service volume (SSV):** The SSV of an NDB depends on what the NDB is being used for. The ranges of NDB SSVs are shown in the Table 2.1. The distances are the same for all heights.
- **Accuracy (2σ):** ± 3 to ± 10 degrees [1].
- **Fix rate:** Continuous [1].
- **System capacity:** Unlimited [1].
- **Advantages:** The advantages of NDB is that it is relatively simple and low cost, and not limited to LOS operation as it operates in the medium radio frequency band.

2.2 VHF OMNIDIRECTIONAL RANGE (VOR)

VHF Omnidirectional Range (VOR) is a navigation aid commonly used in aeroplanes for navigation. It is an old technology that has been around since the late 1940s. The VOR transmitter is a ground beacon that transmits the following three signals [30]:

1. The Morse ID of the VOR ground beacon; transmitted every 10 seconds.
2. A reference signal repeated at 30 Hz.
3. A directional signal, with its phase compared to the reference signal being proportional to the azimuth angle. This is rotated at 30 Hz.

The reference signal is omnidirectional and radiates outwards in a circular pattern from the ground station. The directional signal rotates uniformly at 30 Hz [1]. A phase difference of zero, between the two signals, indicates that the aircraft is on the zero radial of the station, i.e., the line going from the beacon through the aircraft points to magnetic north (see Figure 2.6).

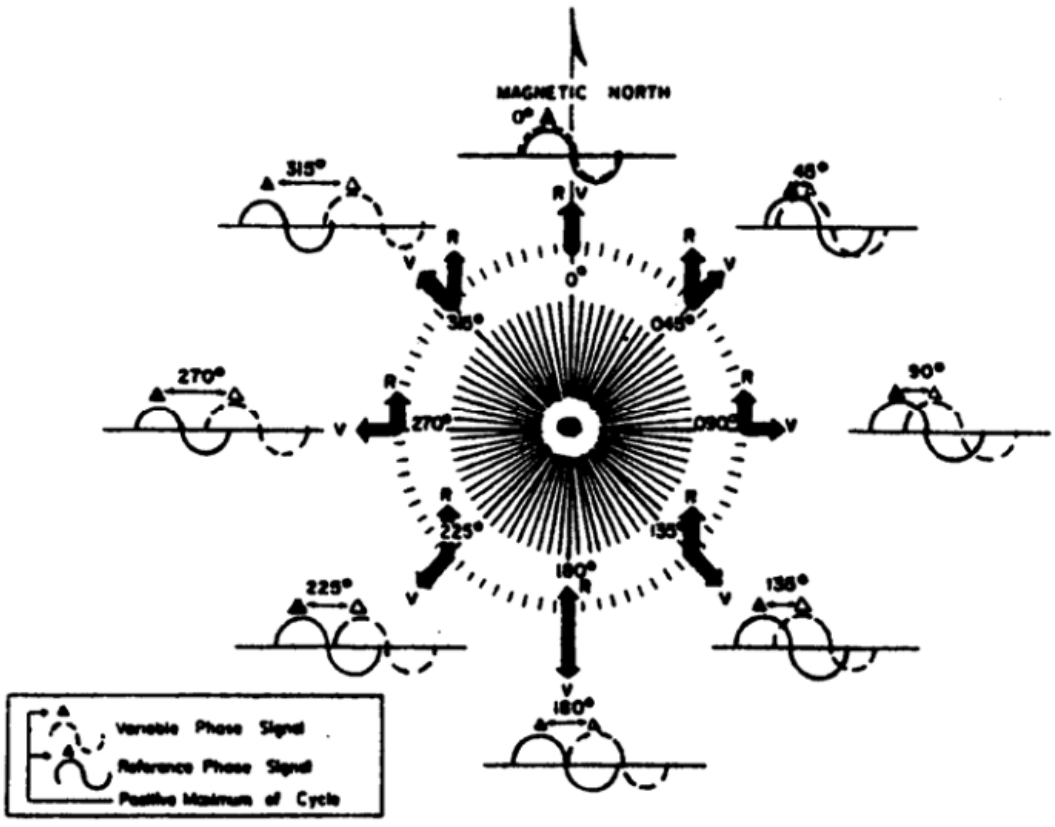


Figure 2.6 VOR phase relationship [14, pg. 7].

The aircraft has a database with the coordinates of all the VOR ground stations. Hence, from the Morse ID the pilot can determine which beacon is transmitting the

signals and where the beacon is situated. By measuring the phase difference between the reference and directional signals the aircraft can determine what radial of the beacon it is on [14]. Since VOR is commonly equipped with a Distance Measuring Equipment (DME), described in Section 2.3, the aircraft is also able to determine its distance from the ground beacon. Having both bearing and distance enables the pilot to obtain a unique position fix on a map.

VOR operates in the VHF band with frequency ranging from 108–117.95 MHz [30]. Hence, its operation is limited to line-of-sight (LOS) which is typical of VHF transmission. This is illustrated in Figure 2.7.

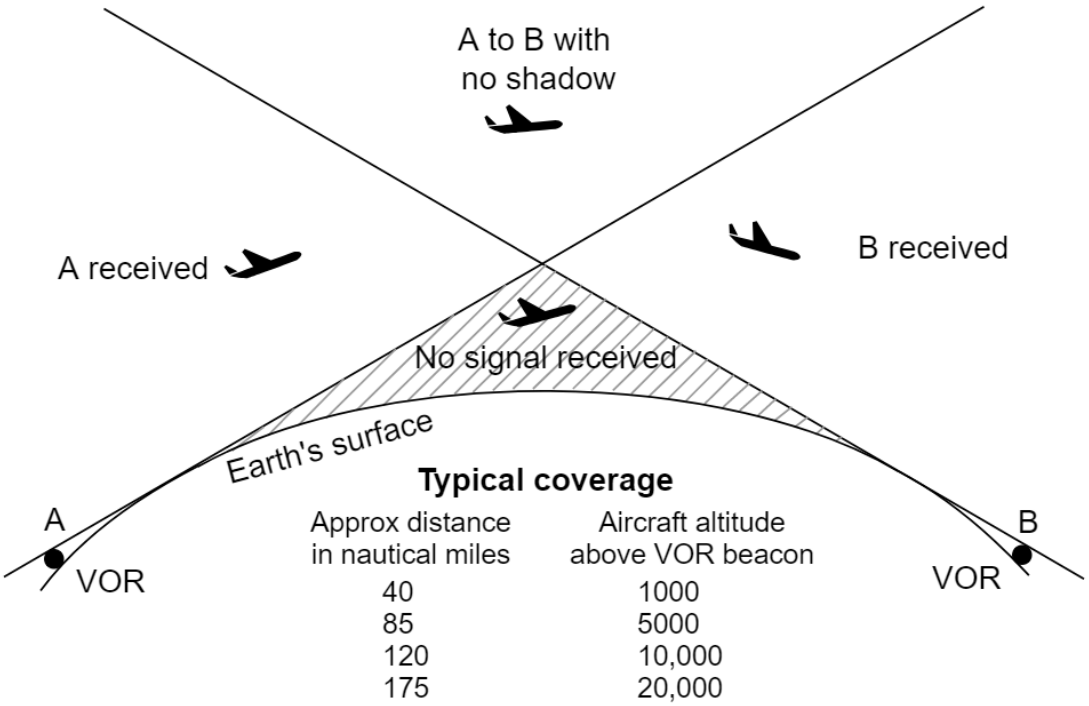


Figure 2.7 VOR Coverage [14, pg. 3].

2.2.1 Airborne Equipment

Onboard the aircraft the equipment required for VOR includes [14]:

1. V-type dipole antenna; horizontally polarised [10].
2. Control box containing an ON-OFF switch, frequency selector, and an aural volume tuner.
3. Conventional superheterodyne receiver.
4. Navigation circuit which takes the received signals and determines the phase difference and hence radial.

Figure 2.8 shows an example of a VOR receiver. There are several variants of varying complexity.

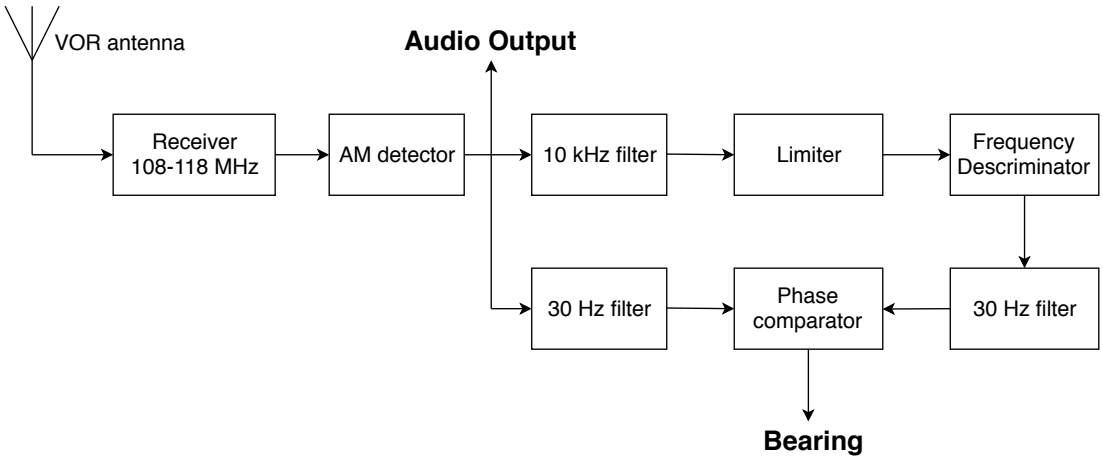


Figure 2.8 Block diagram of a standard analog VOR receiver. The phase difference of two 30 Hz waveforms is used to determine the VOR radial, and a 1020 Hz tone encodes the Morse ID of the VOR ground beacon [43].

2.2.2 Characteristics

- **Accuracy:** The radial determination of a Conventional VOR (CVOR) system is accurate, 99.7% of the time, to ±5.6° for an airline type receiver [11]. There are many errors that contribute to the this; the major cause being ground station error, which is greater than the next 9 errors combined.

  In CVOR the reference signal is sub-modulated in FM and the directional signal is sub-modulated in AM [30]. A more advanced system is known as Doppler VOR (DVOR), where the reference signal is sub-modulated in AM, and the directional signal in FM. As a result it has a higher prescribed accuracy of ±1.4° due to better robustness to disturbances offered by the frequency sub-modulated directional signal [30].

- **Range:** VOR stations serve a volume of airspace around the VOR station called its standard service volume (SSV). Some stations serve small regions out to 25 NM — known as terminal VORs (T-VOR). Others serve greater regions out to 130 NM. These VORs are only different in that their power outputs have been adjusted to provide adequate signal strength within their SSV. VOR signals within a particular SSV should not experience interference from signals from other VOR stations on the same frequency [46].

  In the U.S, there are three standard service volumes: terminal, low, and high. Table 2.2 outlines the SSVs applicable to VOR, DME, and TACAN.

SSV Class Designator	**Altitude and Range Boundaries**
T (Terminal)	From 1,000 feet above ground level (AGL) up to and including 12,000 feet AGL at radial distances out to 25 NM.
L (Low altitude)	From 1,000 feet AGL up to and including 18,000 feet AGL at radial distances out to 40 NM.
H (High Altitude)	From 1,000 feet AGL up to and including 14,500 feet AGL at radial distances out to 40 NM. From 14,500 feet AGL up to and including 60,000 feet AGL at radial distances out to 100 NM. From 18,000 feet AGL up to and including 45,000 feet AGL at radial distances out to 130 NM.

Table 2.2 VOR/DME/TACAN standard service volumes (SSV) [46].

- **Capacity:** The capacity of a VOR station is unlimited [1].
- **Fix rate:** Continuous update rate of 30 updates per second [1].
- **Cost:** See Appendix C.

2.3 DISTANCE MEASURING EQUIPMENT (DME)

DME is a transponder based radio navigation technology that measures slant range, between an aircraft and ground station, by timing the propagation time of a UHF radio signal from the aircraft to the ground station and back. It is a secondary radar, but in reverse. The DME interrogator (on the aircraft) transmits a pulse pair which is received by the transponder (ground station). The transponder waits for a predetermined amount of time and then transmits a pulse pair of its own in response [12].

All pulses have the duration of 3.5 μs [12].

Slant range can be measured using the following equation:

$$s = ct\,, \tag{2.1}$$

where,

- c is the signal propagation speed, and
- t is the pulse pair propagation time to the transponder and back minus the transponder delay time, all divided by two, i.e,

$$t = \frac{\text{round trip time} - \text{transponder delay}}{2}\,. \tag{2.2}$$

DME operates in the ultra high frequency (UHF) band, with 252 channels contained in the 962–1213 MHz frequency band. The interrogator transmit frequency is within the 1025–1150 MHz band, whereas the transponder transmit frequency is within the 962-1024 MHz band and 1151–1213 MHz band. There are a total of 252 channels; 126 for interrogations, and 126 for replies. The interrogation and reply frequencies always differ by 63 MHz [12].

Channels are numbered from 1 to 126. Each numbered channel is further divided in to X and Y channels. Each numbered pair of channels is separated from the adjoining pair by 1 MHz [12]. Though each channel is 1 MHz wide the signal spectrum is only 100 kHz [48].

X and Y channels are distinguished from one another by their different pulse separation times. All X channels have the same pulse separation time of 12 μs for both the interrogator and transponder. For Y channels the pulse separation time of 36 μs for the interrogator and 30 μs for the transponder [12]. This is illustrated in Figure 2.9.

Since DME ground beacons are co-located with VOR/ILS beacons, DME channels are paired with VOR/ILS channels [46]. Hence, by selecting a VOR/ILS channel the corresponding DME channel is selected automatically. Table 2.3 shows this pairing arrangement [12].

DME exchanges pulse-pairs with the ground beacon using two modes of timing:

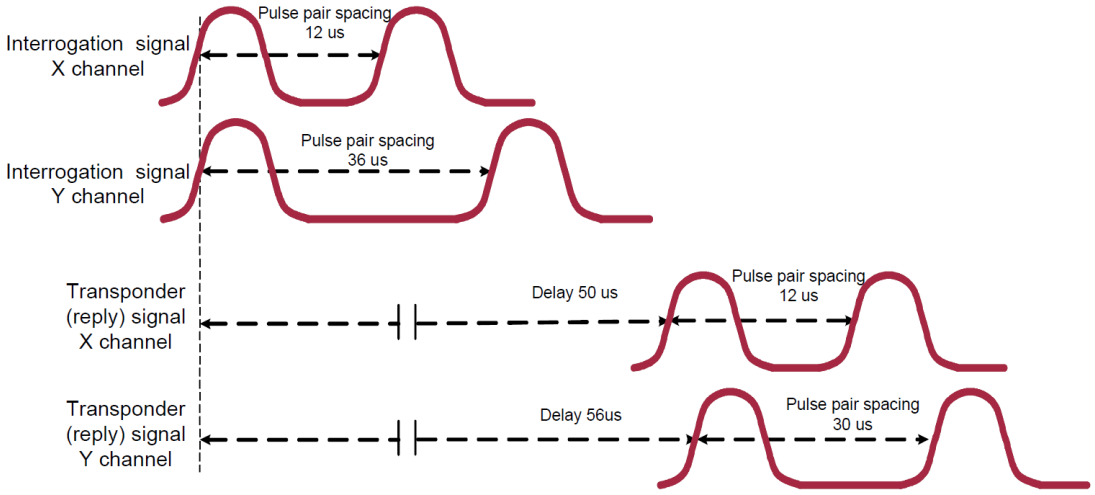


Figure 2.9 DME X and Y channel pulse spacing [32].

	TACAN/DME Channels									
VOR FREQ (MHz)	.00	.10	.20	.30	.40	.50	.60	.70	.80	.90
108	17	18	19	20	21	22	23	24	25	26
109	27	28	29	30	31	32	33	34	35	36
110	37	38	39	40	41	42	43	44	45	46
111	47	48	49	50	51	52	53	54	55	56
112	57	58	59	70	71	72	73	74	75	76
113	77	78	79	80	81	82	83	84	85	86
114	87	88	89	90	91	92	93	94	95	96
115	97	98	99	100	101	102	103	104	105	106
116	107	108	109	110	111	112	113	114	115	116
117	117	118	119	120	121	122	123	124	125	126
133	-	-	-	60	61	62	63	61	65	66
134	67	68	69	-	1	2	3	4	5	6
135	7	8	9	10	11	12	13	14	15	16

Table 2.3 VOR/DME channel pairing.

1. **X Mode**: When the control box is channelled to a frequency ending in .X0, e.g. 108.00 or 128.70, the DME is operating in X-Mode [1]. Here the interrogation pulses are separated by 12 μs, the reply pulses are also separated by 12 μs, and the transponder delay time is 50 μs [32].

2. **Y Mode**: When the control box is channeled to a frequency ending in .X5, e.g. 116.55 or 130.05, the DME is operating in Y-Mode [1]. Here the the interrogation pulses are separated by 36 μs. The reply pulses are separated by 30 μs, and the transponder delay time is 56 μs [32].

The purpose of the transponder delay (50 μs in X-mode) is to eliminate the possibility of uncoordinated operation when the aircraft is close to the transponder [22].

The Morse ID of the DME transponder is the same as the Morse ID of the parent facility (i.e., the VOR/ILS station), except that the Morse ID of the DME is transmitted once for every 3 to 4 transmissions of the parent facility ID; approx. once every 40 seconds [32]. It is also transmitted in between successive VOR ID transmissions. Additionally DME IDs are transmitted at 1350 Hz [46], which is higher pitched than the 1020 Hz Morse ID that is used for VOR.

2.3.1 Modes of Operation

- **Standby mode:** When the system is powered up, it enters Standby Mode. The receiver and audio are operative, but the transmissions are inhibited. The DME display shows four dashes, indicating that no distance measurement has been computed. The receiver monitors the received pulse pairs and if sufficient pulse pairs have been counted it enters Search Mode [22].

- **Search mode:** In Search Mode the interrogator attempts to synchronise and set up a connection with the ground station. In this mode, the interrogator may transmit up to 150 pp/s until it receives a specific number of reply pulses [32]. Once connected and synchronised, it enters Track Mode.

- **Track mode:** In Track Mode, distance measurements are performed at regular intervals, and the interrogation rate is reduced, freeing up band space for other airborne DMEs [22]. The maximum rate in this mode is 16 pp/s. The slant distance is displayed on the DME indicator. Figure 2.10 shows a typical DME indicator.

- **Memory mode:** If no pulse-pairs are received after a short time ($\sim$2 s) then the DME goes into Memory Mode where distance is calculated based on the previous received distance. Memory Mode expires after about 10 s; afterwards the DME goes into Search Mode.

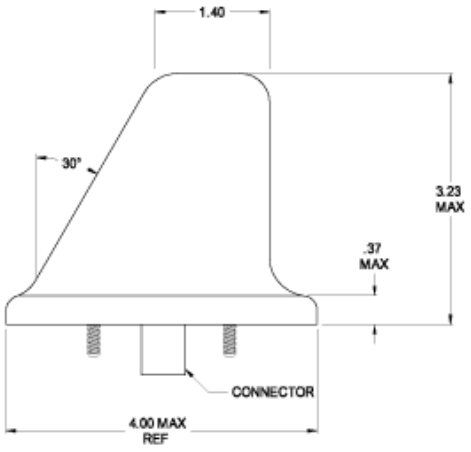
Figure 2.10 Typical airborne DME display, [22]. The monitor shows the slant range in nautical miles, and the channel frequency of the parent facility, which in this case is VOR, in MHz.

If the average ground beacon transmit rate drops below 700 pp/s, e.g., due to low numbers of aircraft in the vicinity, the ground station will add randomly spaced "squitter pulses" to ensure a minimum pulse rate is provided. This minimum pulse rate ensures that the aircraft receiver's automatic gain control (AGC) can synchronise with the signals of the ground station. There is also a built in test equipment inside the transponder which requires a minimum pulse rate, i.e., test pulses, in order to operate properly. These random squitter pulses are generated by a local interrogator located inside the ground station. When the pulse rate drops below the minimum, the local interrogator sends pulse-pairs to the transponder, which processes them exactly like aircraft interrogations [32].

2.3.2 Airborne Equipment

In order to use DME both the ground station and aircraft need an UHF transmitter and receiver. Figure 2.11 shows a DME antenna. The antenna is mounted on the underside of the fuselage. The dimensions of the antenna are shown in Figure 2.11b.

(a) Physical antenna.



(b) Antenna dimensions in inches.

Figure 2.11 CI-105 shark fin 1/4 wave DME antenna by Comant. Antenna is vertically polarised.

When banking the aircraft, the antenna may be shielded from the ground station. In such a case the DME enters Memory Mode, instead of showing an error or no distance.

A DME block diagram is shown in Figure 2.12.

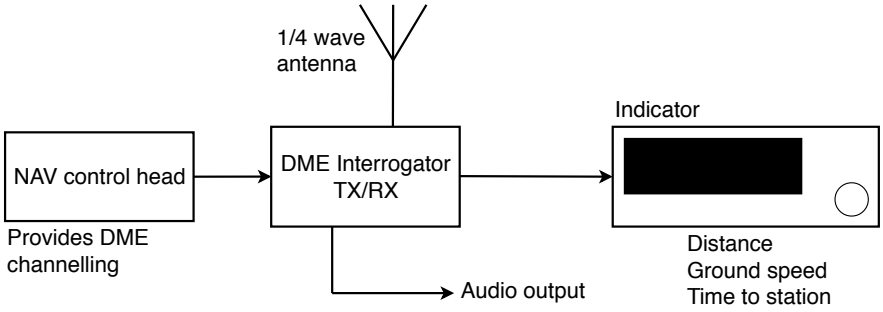


Figure 2.12 DME system block diagram [22].

2.3.3 Characteristics

- **Capacity:** The ground station can accommodate about 110 aircraft at a time [1]. Above this, the ground station will limit the number of interrogations by reducing the receiver gain, ignoring more distant aircraft [22].
- **Accuracy (2σ):** The DME system must be designed such that the overall system error is not more than $\pm 0.5\,\text{NM}$ or $3\,\%$ of the calculated range, which ever is greater [1].
- **Range:** Since DME operates in the UHF band, it is limited to line-of-sight operation. The SSV of DME is identical to that of VORs since they are usually co-located. See Table 2.2 in section 2.2.
- **TX Power:** The transmit power of an aircraft interrogator is minimum $250\,\text{W}$ [32].
- **Fix rate:** Update rate varies with the design of the airborne equipment and system loading; it is typically 10 per second [1].
- **Cost:** See Appendix C.
- **DME Errors:** Time-to-station and time-from-station is accurate only if the aircraft is moving directly towards or away from the station [3]. The same applies to ground speed. When moving in any other direction the reported ground speed is erroneously low and time-to-station erroneously high.

  The distance shown on the DME monitor is taken as the horizontal distance between aircraft and ground station, whereas it is actually the slant range. This error is smallest at low altitudes and at long ranges from the ground station, but greatest when the aircraft is directly above the station where the reported distance is the height above the station and the horizontal distance is zero. This error is

negligible if the aircraft is greater than 1 mile from the ground station for every 1,000 feet in altitude above the station [3].

Some DMEs correct this by using altitude to calculate the actual horizontal distance [3].

Ground speed and time-to-station is calculated based on horizontal distance which is assumed to be equal to slant range. This results in large errors when close to the station for both ground speed and time-to-station.

2.4 CELLULAR POSITIONING METHODS

The following subsections will describe the positioning technologies of 2nd generation (2G), 3G, and 4G cellular networks. Only cellular technologies available in New Zealand will be explored.

2.4.1 GSM/GPRS/EDGE (2G) Location Services

The GSM/GPRS/EDGE Location Services (LCS) architecture has three positioning methods:

1. Cell ID and Timing Advance (CID + TA).
2. Enhanced Observed Time Difference (EOTD).
3. Uplink Time Difference of Arrival (UTDOA).

2.4.1.1 Cell ID and Timing Advance

This is a centroid based positioning method. Pure CID only returns the coordinates of the serving cell sector as the MS location. Its accuracy is limited to the size of the cell which in GSM can be up to 35 km in radius [2].

By using the TA parameter the MS can bound its positioning error to an annular of width 554 m [2]. The TA parameter has a granularity of one bit period (∼3.69 s) equating to a distance of 1107 m [2]. Since this is equal to the RTT, diving it by two gives ∼554 m (the one way distance between the UE and the BTS). The TA parameter is originally used to align the uplink transmissions of all MSs within a sector [16]. By obtaining the CID and TA values from at least 4 different BTS the MS can obtain a unique 3-dimensional position fix via circular trilateration.

2.4.1.2 Enhanced Observed Time Difference

EOTD is a hyperbolic trilateration method which relies on time difference of arrival measurements to localise the MS. There are two types of EOTD in the GSM/GPRS/EDGE RAN (GERAN) [16]:

1. MS-assisted: the MS send measurements to the Serving Mobile Location Center (SMLC, i.e., the network) to calculate the MS's position.
2. MS-based: the MS calculates its position itself based on measurements it obtained itself and assistance data broadcast by the network.

The issue with EOTD in GERAN is that the BTS are not time synchronised. This means that the positioning signals which the MS uses for TDOA are not transmitted at the same time from each BTS. To solve this issue GERAN employs Location Measurement Units (LMUs) which measure the time difference between the signals transmitted by different BTS [16].

In this method, the MS records the time of arrival (TOA) of pilot signals transmitted from at least four BTSs. It then calculates the difference between these TOAs which are known as observed time differences (OTDs). Three unique OTDs can be obtained from the TOA of four different BTS. This is sufficient for a unique position fix.

These time differences do not account for the time discrepancy, T_d, between the clocks of the BTS. The LMUs measures this time discrepancy. The real time difference, RTD, is obtained using the equation: $\text{RTD} = \text{OTD} - T_d$.

In MS-assisted EOTD, the MS measures the OTD values and the LMU measures the T_d values. Both the MS and the LMU send this data to the network (through the BTSs). Using this information the network is able to calculate the location of the MS.

In MS-based EOTD, the MS measures OTD values and the LMUs measures the T_d values. The LMU sends its T_d measurements to the network, then the network sends these measurements plus other assistance data to the MS so that it can calculate it position.

No accuracy data was available for this method.

2.4.1.3 Uplink Time Difference of Arrival

UTDOA is also a hyperbolic multilateration positioning technique, but it is a purely uplink method, i.e., network based.

In UTDOA a signal is transmitted by the MS and the TOA of this signal is measured by at least four LMUs. Because all LMUs are equipped with GNSS modules, they all share the same clock reference. Hence, the time difference of arrival (TDOA) of these signals can be measured between pairs of LMUs [16].

The LMUs transmit these measurements to the BTSs which then pass it on to the network. The network calculates the TDOA of these signals. The results are then applied to a hyperbolic multilateration algorithm to calculate the position of the MS. The network then sends this information back to the MS to make it aware of its location.

The advantages of this method are [16]:

- No software updates are required at the MS for making measurements, reporting measurements, or calculating its position.
- The ability to locate any terminal, regardless of any built-in hardware features or software updates, is particularly important in scenarios like emergency call localization.

The disadvantages of this method are [16]:

- Requires the deployment of more geographically dispersed LMUs.
- All LMUs must have a common clock reference, i.e., all must be equipped with GNSS receivers.
- Exchange of coordination messages between the serving BTSs and the LMUs generates extra signalling load in the network.

No accuracy data was available for this method.

2.4.2 UMTS (3G) Location Services

GSM/GPRS/EDGE and UMTS networks have completely different RANs but share most core network elements. The UMTS LCS architecture has three positioning methods:

1. Cell ID.
2. Observed Time Difference of Arrival with Idle Periods in the Downlink (OTDOA-IPDL).
3. Uplink Time Difference of Arrival (UTDOA).

2.4.2.1 Cell ID

This is a proximity based positioning method, as it returns the coordinates of the serving cell as the location of the MS. These coordinates might be the location of the NodeB antennas, or the centre of the cell [16]. The accuracy of this method is equal to the size of the cell which can be as large as tens of kilometres in radius.

2.4.2.2 Observed Time Difference of Arrival with Idle Periods in the Downlink

CDMA and WCDMA can suffer from a condition known as the "near-far" effect, where the reception at the UE of strong signals from a nearby NodeB make it impossible to detect and demodulate signals from more distant NodeBs [16]. Because all cells share the same downlink frequency, in the reception of signals from a given cell the energy sum of signals from all other cells act as noise. If the signal of a nearby NodeB is received with a high energy, the SNR of a distant NodeB will be low [16].

To implement a positioning systems using hyperbolic multilateration, the UE must obtain TOA signals from at least four different NodeBs. The near-far effect could make these measurements unattainable or attainable only at cell borders.

To prevent this issue UMTS uses Observed Time Difference of Arrival with Idle Periods in the Downlink (OTDOA-IPDL). During an idle period, a cell will transmit only the synchronization signal or nothing at all, depending on the idle period configuration — continuous mode or burst mode. The idle periods of the serving cell are used to receive synchronisation signals from other NodeBs; maximising the hearability of signals from distant NodeBs. The UE knows when the idle periods occur [36].

An enhancement of OTDOA-IPDL is called OTDOA with TA-IPDL (time-aligned idle periods in the downlink). Here the idle period is used for all NodeBs to send a signal that can only be used for location estimation. This helps to enlarge the accuracy but also brings more complexity to the network and reduces the communication efficiency. This is because during the idle-periods all NodeBs are busy transmitting the positioning signal — leading to network capacity loss [36].

To reduce this capacity loss that results from IPDL, an alternative method called Cumulative Virtual Blanking (CVB) can be used. This is where the Serving Mobile Location Centre (SMLC) does some digital signal processing to the transmitted signals to remove stronger signals consecutively — making it easier for the UE to extract the timing signal from the weaker signals. This has comparable results to IPDL [36].

A fundamental aspect of WCDMA network planning is that the serving cell must have a dominant area where its signals must overcome signals from neighbouring cells. Hence, although OTDOA-IPDL improves TDOA availability it is still difficult to obtain at least four TOA measurements. Simulations from [16] show that OTDOA-IPDL improves OTDOA availability from 31% (with no idle periods) to 74% (with idle periods). This is a significant improvement but still insufficient for a reliable positioning system.

The accuracy of regular OTDOA, with no IPDL, according to [38] is 50–150 m in urban areas and a few kilometres in rural areas. No information was found on the accuracy of OTDOA-IPDL.

2.4.2.3 Uplink Time Difference of Arrival

UTDOA positioning in 3G networks is done the same way as in 2G networks. See section 2.4.1.

The accuracy of UTDOA is <50 m in urban areas according to [38] and requires the deployment of GNSS synchronised LMUs. No accuracy information was found for rural areas.

2.4.3 LTE (4G) Location Services

The LTE/LTE-A LCS architecture has three positioning methods:

1. Cell ID and Timing Advance (CID + TA).

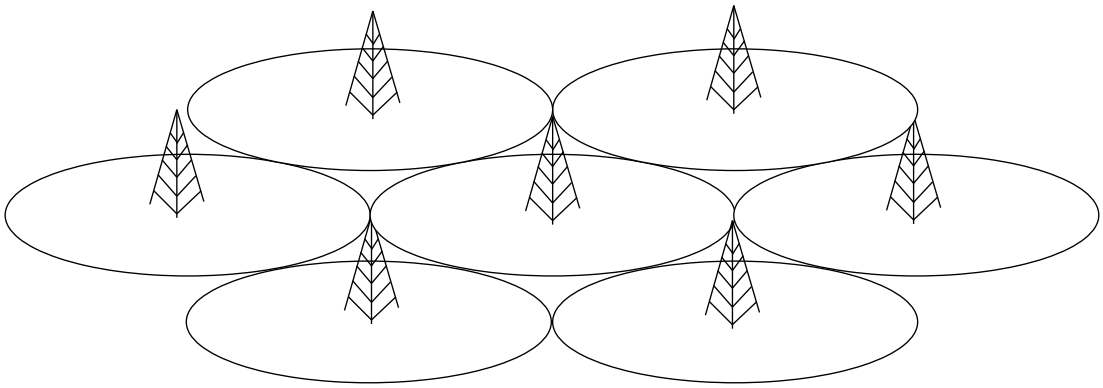


Figure 2.13 LTE cell structure. The circular regions are known as cells; all UEs within a cell are served by the eNB located at the centre. Each eNB usually has three antennas; each antenna serving one sector of the cell. A sector is often a 120 degree sector of a cell.

2. Observed Time Difference of Arrival (OTDOA).

3. Uplink Time Difference of Arrival (UTDOA).

2.4.3.1 Cell ID and Timing Advance

Each eNB (LTE base-transceiver station) has a region called a cell (see Figure 2.13) in which it transmits its signals and serves the UEs (LTE mobile stations) within that cell. The eNB of each cell is given a unique cell ID by the network; in LTE this is usually a six digit integer. When a UE connects to an eNB it receives the cell ID of that eNB. By associating a co-ordinate with each cell ID the UE is able to determine what cell it is in. Usually these coordinates are the coordinates of the eNB which is likely to be at the centre of the cell.

CID positioning is the coarsest positioning method in any cellular network with the accuracy being limited to the size of the cell. Although Figure 2.13 shows each cell as equal in size, in practice this is not the case. The size of a cell is typically determined by the expected number of users within that region. In densely populated areas (e.g., urban) the cell size can be a few hundred metres or less in radius, whereas in rural areas it may have a radius up to tens of kilometres.

The accuracy of CID based positioning (in LTE) can be improved by utilising the Timing Advance (TA) value, described in Section 3.1, that is measured by the eNB and provided back to the UE. The TA value is a measure of the round trip time (RTT) between the UE and eNB originally used for aligning the uplink transmissions of UEs within a cell. The TA value has a granularity of $0.52\,\mu$s — equating to 156 m [33]. Dividing this by two for a single sided trip yields a positioning accuracy of 78 m. The maximum TA value of 1282 equates to a propagation distance of $\sim$100 km, hence it would be able to facilitate a cell radius up to $\sim$100 km [33].

2.4.3.2 Observed Time Difference of Arrival

In LTE release 9 the Positioning Reference Signal (PRS) was introduced. It is broadcast on antenna port 6; an antenna port is a logical mapping of OFDMA channels, rather than a physical antenna. It is designed for positioning only, hence conveying no high level information, and existing only at the physical layer [16].

The PRS of a certain cell is configured to correspond to empty resource elements in neighbouring cells, enabling high signal to interference ratio (SIR) conditions when receiving neighbour cell PRSs [19].

The accuracy of this method is claimed to be 50–200 m based on simulation performed by [39]. [21] claims theoretical accuracy of <100 m.

2.4.3.3 Uplink Time Difference of Arrival

UTDOA is essentially OTDOA in reverse. The positioning method is based on the Sounding Reference Signal (SRS) [21] transmitted from the UE and received by at least four different eNBs. Three time differences are calculated based on these measurements and a hyperbolic multilateration algorithm is used to find the location of the UE.

According to [21] UTDOA should have a theoretical accuracy of <100 m ("only for large bandwidths and only with special processing in the receiver").

2.5 TRADE-OFF ANALYSIS

A comparison of all of the positioning technologies (both existing and potential) discussed earlier in this chapter are presented in Table 2.4. Based on the information in this table and other suitable information the most suitable position technology will be selected and further tested in the subsequent chapters.

The accuracy of DME is ±0.5 NM (±926 m) or 3 % of the total distance; whichever is greater (see Section 2.3). This indicates that the accuracy of DME is limited to a minimum of ±926 m which is very poor. Its coverage is shown in Figure 2.15 which almost covers the entirety of New Zealand.

The accuracy of NDB is specified as ±3 ° to ±10 °; see Section 2.1.1. Consider the equation,

$$s = r\theta, \tag{2.3}$$

where

- r is the straight line distance of the UAV from the ground station,
- θ is the angular error (in radians) representing the accuracy of the navigation aid (navaid), and
- s is the arc length representing the accuracy of the navaid in metres.

Based on Equation 2.3, when the UAV is at a distance $r = 954$ m from the NDB ground station, taking the best case accuracy of 6 ° (±3 °), the ambiguity in the position of the UAV is a arc of length 100 m. This calculation shows the the accuracy of NDB quickly degrades as the UAV moves away from the ground station.

Using the same equation (2.3) for CVOR, at a distance of $r = 511$ m, and accuracy of $\theta = 11.2$ ° (±5.6 °), the ambiguity in the position of the UAV is an arc length of 100 m.

Using the same equation (2.3) for DVOR, when the UAV is $r = 2046$ m from the DVOR ground station, using an accuracy of $\theta = 2.8$ ° (±1.4 °), the ambiguity in the position of the UAV is an arc length of 100 m.

Although VOR provides great coverage in New Zealand (almost 100 % coverage above 14,500 ft AGL; see Figure 2.14), for the majority of the UAV's flight the UAV will likely be much further than 2046 m from the ground station due to the low number of VOR ground stations (see Table 2.5). Hence, the accuracy of CVOR/DVOR will mostly be unsatisfactory, and even worse for NDB.

2G is a very old cellular technology and will soon be phased out. Out of the three major mobile service providers in New Zealand, only Vodafone currently provides GSM services [47]. Spark and 2degrees have already phased it out. [26] shows a list of dates

	NavAids	Accuracy	Precision (%)	Coverage	Capacity	Update rate	Notes
	CVOR	±5.6° ±1° in airline types RX	99.7	1000-12000ft AGL: 25 NM	∞	30 Hz	- LOS; could mean no signal at low altitude. - Sector length, l = rθ. Large r gives less accuracy.
	DVOR	±1° ±0.4° in airline type receivers.	99.7	1000-18000ft AGL: 40 NM 14500-60000ft AGL: 100 NM			
	DME	0.5 NM or 3% of range; whichever is greater.	95	18000-45000ft AGL: 130 NM DME Max = 200 NM	Typ. 100 users (min 50).	25 Hz (track mode)	- LOS (UHF). - TX requires approval. - Range ambiguity when close to beacon
	NDB	min ±5°	95	Depends on NDB type. Compass Locator: 15 NM MH: 25 NM H: 50 NM HH: 75 NM	∞	Continuous	- Non-LOS - Low cost - Night effect - Co-channel interference - Terrain effect - Thunderstorm effect
GSM/ GPRS/ EDGE (2G)	CID+TA	554 m		urban: high rural: med-low			
	EOTD	No info			∞		Requires GNSS synchronised LMUs
	UTDOA	No info					
UMTS (3G)	Cell ID	Size of cell		Urban: high Rural: med-low			
	OTDOA - IPDL	No info			∞		
	OTDOA (no IPDL)	urban: 50-100 m. Rural: a few km.					
	UTDOA	<50 m					Requires GNSS synchronised LMUs
LTE (4G)	CID+TA	78 m theoretical.		Urban: high Rural: med-low			
	OTDOA	50-200 m based on simulation.			∞		
	UTDOA	<100 m theoretical (for large BW)					

Table 2.4 Table comparing the accuracy, capacity, coverage, and update rate of various positioning technologies. Cellular technologies have not been used for positioning very much or at all previously, hence, a lot of the boxes are empty.

NDB/DMEs	NDBs	DMEs	VOR/DMEs
Alexandra (LX)	Ashburton (AS)	Mt Mary (RY)	Auckland (AA)
Henley (HL)	Berridale (BE)	Ohura (OR)	Christchurch (CH)
Hokitika (HK)	Cape Campbell (CC)	Tory (TR)	Gisborne (GS)
Kaitaia (KT)	Chatham Islands (CI)		Hamilton (HN)
KeriKeri (KK)	Ferry (FY)		Invercargill (NV)
Manapouri (MO)	Great Barrier (GB)		Napier (NR)
Paraparaumu (PP)	Hamilton (HN)		Nelson (NS)
Taupo (AP)	Kaikoura (KI)		New Plymouth (NP)
Tauranga (TG)	Miranda (RD)		Ohakea (OH)
Timaru (TU)	Mosgiel (MI)		Palmerston North (PM)
Westport (WS)	Newlands (NL)		Queenstown (QN)
Whakatane (WK)	Springfield (SF)		Rotorua (RO)
Whanganui (WU)	Surrey (SY)		Swampy (SW)
Whangarei (WR)	Taumaranui(TM)		Wellington (WN)
	Waiuku (WI)		Whenuapai (WP)
	Wairoa (WO)		Woodbourne (WB)

Legend	
	Operational and owned by Airways
	Whenuapai and Ohakea operational and owned by RNZAF
	Operational and owned by Chatham Islands
	Wairoa NDB is to be withdrawn 10 Nov 2016

Table 2.5 List of New Zealand ground based Navigation Aids [5].

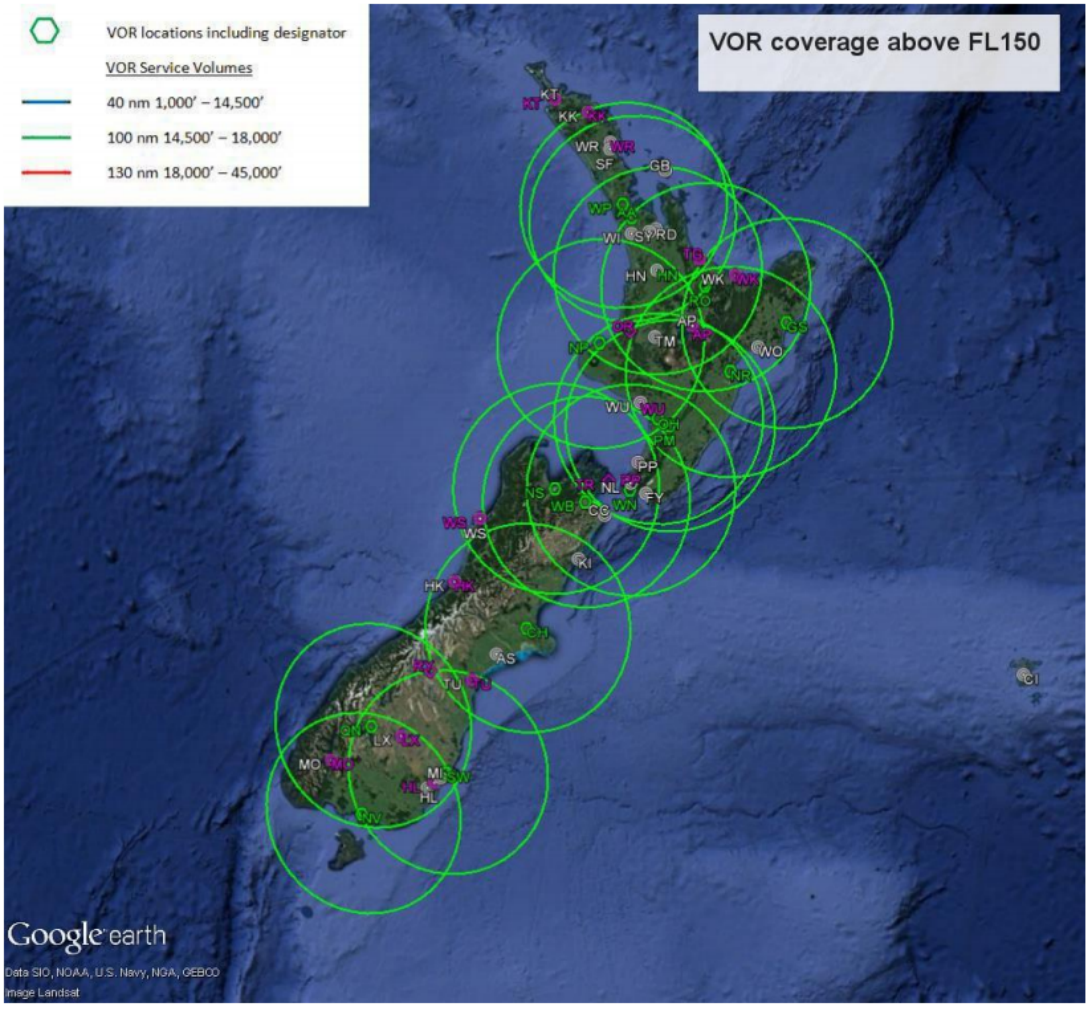


Figure 2.14 VOR coverage above 14,500 ft AGL [5].

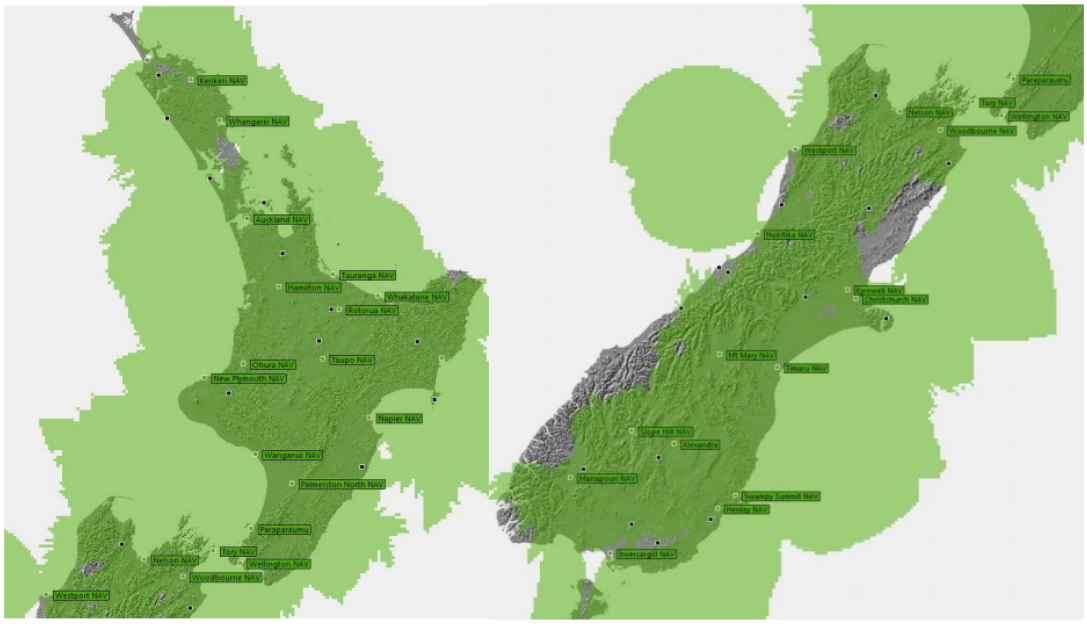


Figure 2.15 DME coverage in the South (left) and North (right) Islands of New Zealand [5].

at which many other countries are planning to shutdown their 2G networks. Hence, 2G will not be explored any further.

The Cell ID positioning method in UMTS is too coarse and will not be considered. The other downlink positioning methods are OTDOA and OTDOA-IPDL. Since these are based on TDOA, the BTS signals must be transmitted at exactly the same time, or the time difference between transmissions must be known. Hence, this will require the deployment of LMUs to measure the time difference between the signals transmitted by different BTS (as done by EOTD in GSM), or the network clocks must be synchronised by GNSS.

UTDOA is the uplink positioning method in UMTS. The issue with this method it that it requires GNSS synchronised LMUs, and generates extra signalling load in the network (reducing overall data throughput). Since GNSS is very widely available, very cheap, and has almost 100 % availability, there's no need for networks to invest in positioning capabilities. Another issue with uplink methods is that the majority of changes are on the network side. hence, unless already implemented by the network, uplink methods are likely infeasible for a masters project, and hence, will not be considered.

Another issue is that 3G networks are relatively old now. Hence, new investments are likely to go solely into 4G systems instead of 3G systems. Thus, unless positioning in 4G LTE is infeasible, 3G UMTS will not explored for positioning.

The LTE positioning methods are:

1. **CID+TA** which has a positioning granularity and theoretical accuracy of 78 m.

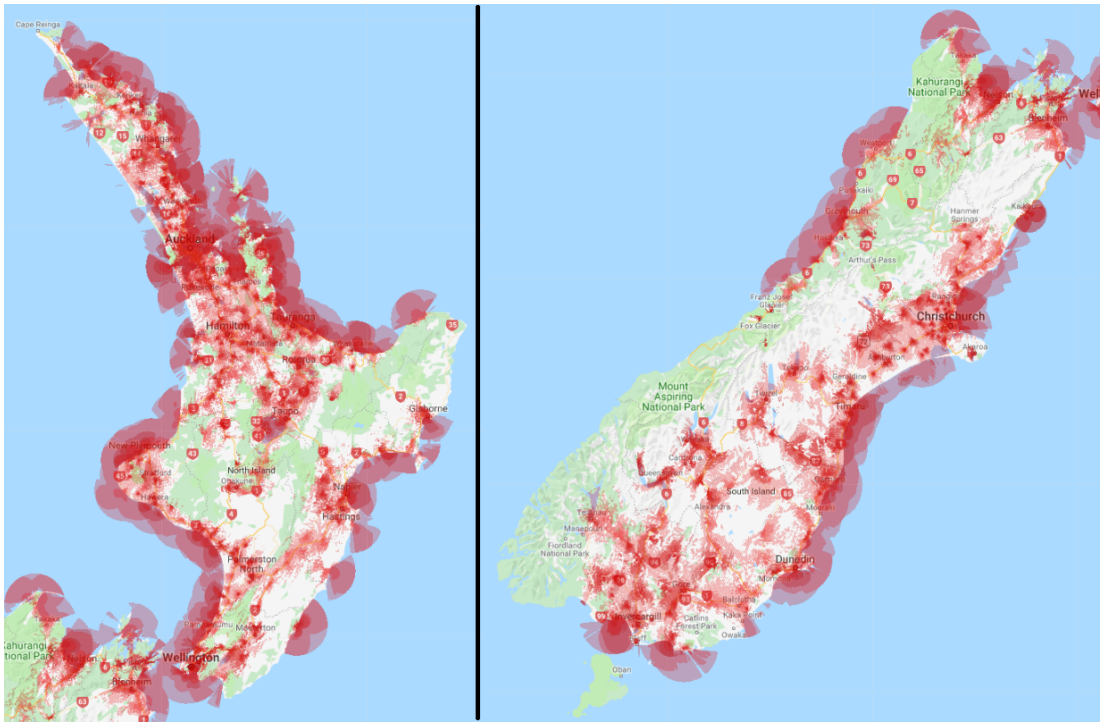


Figure 2.16 Vodafone's 4G LTE coverage in the North (left) and South (right) Islands of New Zealand. Image obtained from `www.vodafone.co.nz/network/coverage/`.

2. **OTDOA** which has a positioning accuracy of 50–100 m based on simulation from [39] and [21] claims a theoretical accuracy of <100 m.

3. **UTDOA** which has a positioning accuracy of <100 m according to [21].

WiMAX[2] is also a 4G technology based on OFDMA but was not considered in this project as it is not deployed in New Zealand. LTE also holds a larger share of the world's 4G market. Hence, regardless of deployment in New Zealand, it is the better option.

Considering that a fully electric VTOL multicopter UAV is designed for short flights (∼1 hour), i.e., mainly to fly within a city or between adjacent cities, it is likely to have LTE coverage for the majority of its flight which both begins and ends in a city. The LTE coverage provided by Vodafone's cell towers is shown in Figure 2.16. The Vodafone network currently has 1324 LTE base stations which provides almost full coverage to the populated regions of New Zealand (see Figure 2.16). Spark and 2degrees, the other Mobile service providers in New Zealand have 1344 and 827 LTE base stations[3] respectively, which should provide even more coverage.

[2]WiMAX: Worldwide Interoperability for Microwave Access

[3]The number of LTE eNBs in service by each network was obtained by counting the number of cell towers that operate at 1800 and/or 700 MHz (frequencies allocated to LTE) from a database of cell towers obtained from `gis.geek.nz`. The 1800 MHz band is also used by GSM in Vodafone so the number of LTE eNBs of Vodafone may be slightly off. Spark and 2degrees do not provide any 2G services.

2.6 CONCLUSIONS

The analysis in section 2.5 shows positioning using VOR, NDB, or DME provide poor accuracy, hence, they will not be explored further.

2G cellular networks are old, and dates have been set by most countries to shut them down [26]. Hence, 2G cellular systems will also be explored no further.

Both 3G UMTS and 4G LTE provide reasonable accuracies based on literature, although UMTS is older than LTE, and will be the first of the two to be phased out. LTE also employs Timing Advance. OTDOA and UTDOA in LTE are part of the LTE technical specifications [4], and hence, is likely to be implemented in actual LTE networks, especially in North America and Europe due to the E911 and E112 mandates respectively. It also provides good coverage in and near the populated regions of New Zealand and will likely be the case elsewhere in the world. LTE also has a higher bandwidth than UMTS, and hence, capable of providing much higher timing resolution.

Therefore all subsequent work will be dedicated to using LTE for positioning. Since the simplest method is Timing Advance, it will be implemented and characterized first, followed by OTDOA and UTDOA.

NOTE: The two subsequent chapters first explore Timing Advance for positioning, and then LTE Signals Of Opportunities (SOP) for positioning. The SOP method was discovered later on in the project after the conclusion of the Chapter on Timing Advance. As a result, in order to ensure the decisions made in this section made sense, the SOP method was not included in the trade-off analysis, or in the literature review. Instead it has a standalone chapter (Chapter 4). Since the SOP method, discovered from [37], claims GPS level accuracy it would not have made sense to explore Timing Advance first (or at all) since its accuracy is worse. Thus, the trade-off analysis which was the reason for selecting LTE (and hence Timing Advance) would not have made sense either.

Chapter 3

POSITIONING WITH LTE TIMING ADVANCE

This chapter will begin by introducing Timing Advance (TA), its purpose in LTE, how it works, and how it can used for localisation. Following that, data will be collected using a commercial available off the shelf (COTS) cellular module. The collected data will then be used to obtain the pseudorange (distance) between the cellular module and cell towers. Then the suitability of TA for positioning will be determined by comparing these pseudoranges with GPS pseudoranges.

3.1 INTRODUCTION TO TIMING ADVANCE

Timing advance is a negative time offset, at the terminal, between the start of a received downlink subframe and a transmitted uplink subframe. By controlling the transmission of uplink subframes the network can make sure that uplink transmissions arrive at the correct time at the eNB (LTE base station). Signals transmitted by multiple terminals within the same subframe, but with different frequency resources (different resource blocks), must arrive approximately time aligned at the eNB so that they do not interfere with signals from other subframes.

In LTE, a terminal is allocated a fixed time window, e.g., a certain number of subframes (1 subframe = 1 ms) in which it has to transmit its uplink data. This is depicted in Figure 3.1 where two time slots are shown; one for user equipment* (UE) 1 and one for UE 2. The network must ensure that UE 1's uplink data arrives at the beginning of its time slot. If this is the case, its transmissions will end before the end of its allocated time slot. But if UE 1 is far from the eNB there will be some propagation delay causing UE 1's uplink transmissions to arrive late, and hence, not at the beginning of its time slot. If its transmissions arrive at T_a, its transmissions could end at T_b (see Figure 3.1), overlapping with the uplink transmissions of UE 2. During the overlap period, UE 1's uplink transmissions will interfere with UE 2's uplink transmissions.

To prevent this, the network sends a TA command which prompts the UE to either

*An LTE mobile station is known as a user equipment (UE) or terminal. Hence, the terms UE and terminal will be used interchangeably.

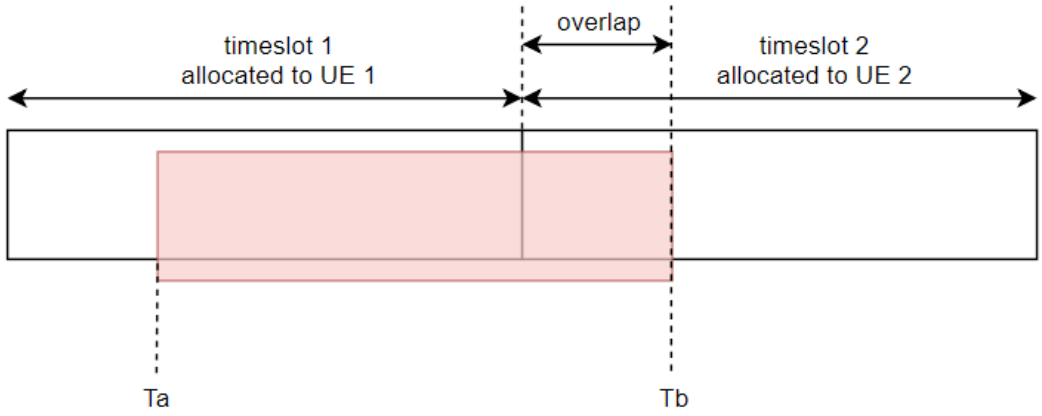


Figure 3.1 Implications at the eNB if uplink transmissions from various terminals (UEs) are not time aligned.

advance or retard its timing relative to its current uplink timing. Figure 3.2 shows a visual representation of what the TA value is.

In Figure 3.2, data from the beginning of subframe (SF) n is sent by the eNB at T_1 and received by the UE at $T_1 + d$ (perceived by the UE as T_1 since the UE does not know the propagation delay). The UE is allocated some timeslot x subframes in the future from T_1 for its uplink transmissions. The UE sends a response at time $T_1 + x \times \mathrm{SF} + d$. Instead of arriving at $T_1 + x \times \mathrm{SF}$ at the eNB, it arrives at $T_1 + x \times \mathrm{SF} + 2d$; which includes both the uplink and downlink propagation delays. By taking the time difference between the start of the allocated subframe ($T_1 + x \times \mathrm{SF}$) and time of arrival of the UE transmissions ($T_1 + x \times \mathrm{SF} + 2d$), the eNB can determine the TA value; which is

$$\mathrm{TA} = (T_1 + x \times \mathrm{SF} + 2d) - (T_1 + x \times \mathrm{SF}) \tag{3.1}$$

$$= 2d\,. \tag{3.2}$$

A TA command, containing the TA value, is then sent to the UE so that it can advance its uplink transmissions by TA seconds.

The TA value for each terminal is measured by the network based on measurements done on each UE's uplink transmissions [19]. Hence, as long as a UE is transmitting uplink data, the network can measure its TA value. The Sounding Reference Signals (SRS) can be used as a regular signal to measure upon [19].

The eNB measures the initial TA value of a UE when it's trying to connect to the network by performing the Random Access procedure via the Physical Random Access CHannel (PRACH). The PRACH is used for uplink transmissions during the UE's initial access, radio link failure, and handover. The eNB sends the TA command in Random Access Response (RAR) [33]. Once the UE is in Connected Mode, the TA

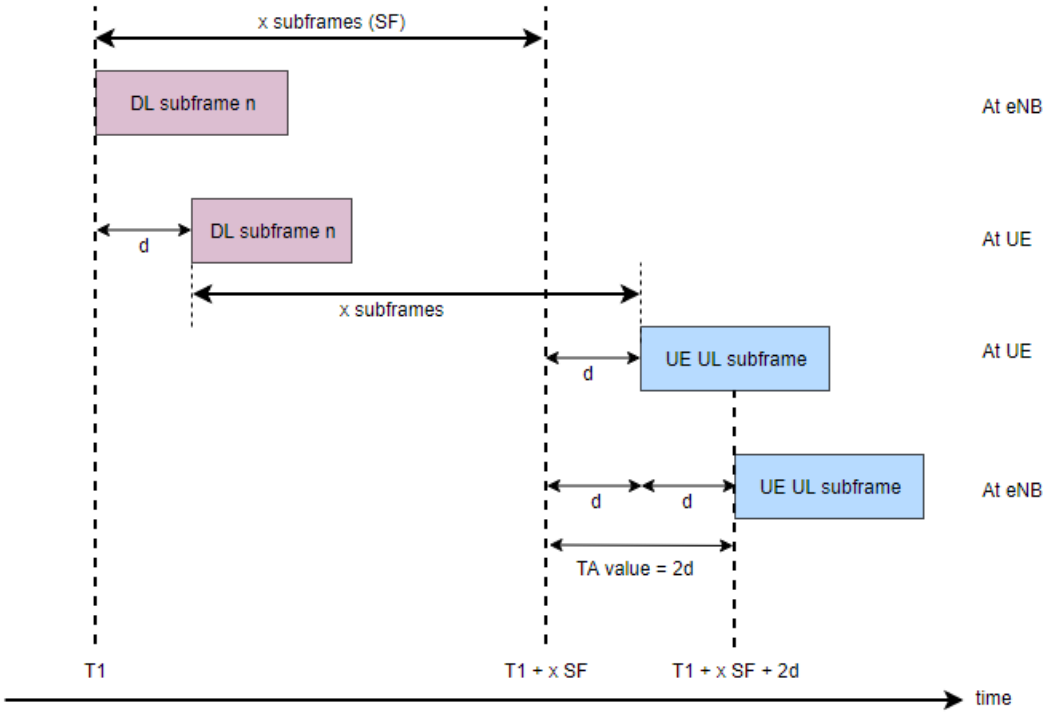


Figure 3.2 Visual representation of how the network calculates timing advance [33].

command is transmitted as a MAC control element on the Down-Link Shared CHannel (DL-SCH) if timing correction is required [19].

The UE must adjust its uplink timing at subframe n+6 for a TA command received in subframe n. Its uplink transmission timing must be adjusted with a relative accuracy of $\leq \pm 4\mathrm{T}_s$ seconds to the signalled TA value compared to the timing of preceding uplink transmissions [33].

The LTE standards specify [9] the following relationship: 1 TA value $= 16T_s \approx 0.52\,\mu$s, where $T_s = 1/(2048 \times 15000) = 1/30720000$ seconds. Hence, a TA value of 1 or $\sim$0.52 μs corresponds to a distance, r, between the UE and eNB, of $\sim$78 m — calculated by the equation:

$$r = \frac{16T_s c}{2}, \tag{3.3}$$

where, c is the speed of light in a vacuum, and the division by 2 yields the one way distance between the UE and eNB.

The following subsections describe how the TA value is communicated to the UE during the Random Access procedure (Section 3.1.1) when the UE is trying to connect to the network and when the UE is fully connected (Section 3.1.2).

3.1.1 TA Command in MAC Random Access Response (RAR)

A MAC Protocol Data Unit (PDU) consists of a MAC header and zero or more MAC Random Access Responses (MAC RARs) and optionally some padding to make up a Transport Block (TB) of a certain size. The MAC header is of variable size.

A MAC PDU header may consist of one or more subheaders. Each subheader corresponds to a MAC RAR; except for the Backoff Indicator subheader. A MAC PDU subheader contains three fields: E/T/RAPID as depicted in Figure 3.3.

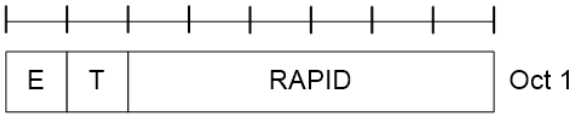


Figure 3.3 E/T/RAPID MAC subheader fields [9].

A MAC RAR contains the following four fields: R/Timing Advance Command/UL Grant/Temporary C-RNTI; as depicted in Figure 3.4.

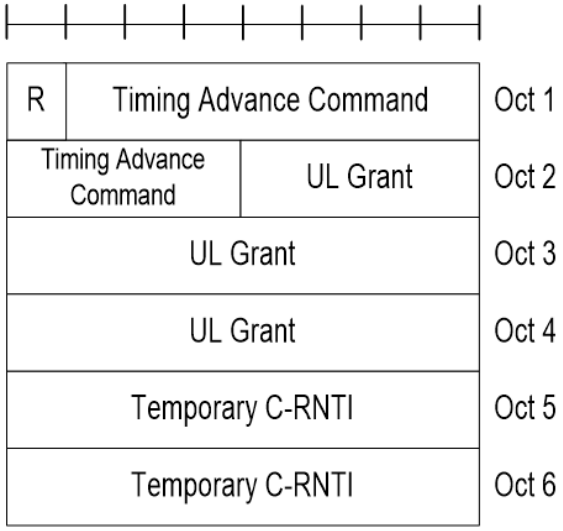


Figure 3.4 Timing advance command in a MAC Random Access Response (RAR) message [9].

The TA value in MAC RAR as shown in Figure 3.4 is 11 bits long, where TA $\in (1, 2, 3, ..., 1282)$. The amount of time alignment is given by $N_{\text{TA}} = \text{TA} \times 16T_s$. The maximum TA value of 1282 corresponds to a delay of $\sim$0.67 ms which corresponds to a distance between the UE and eNB of just over 100 km; $(0.6667 \times 10^{-3} \times 3 \times 10^8)/2 = 100{,}156$ m.

3.1.2 TA Command in MAC Control Element (CE)

The TA command in MAC CE is found in the MAC PDU subheader. It is a single octet (see Figure 3.5). The first two bits contains the Timing Advance Group (TAG)

ID, and the last 6 bits contain the TA value; where TA $\in (0, 1, 2, ..., 63)$. This value is used to control the amount of timing adjustment the MAC entity has to apply. The new timing adjustment, $N_{\text{TA,new}}$ is

$$N_{\text{TA,new}} = N_{\text{TA,old}} + (\text{TA} - 31)16T_s\,, \tag{3.4}$$

where, $N_{\text{TA,old}}$ is the current/old timing adjustment. A positive N_{TA} value requires the current uplink timing to be advanced whereas a negative value requires it to be delayed.

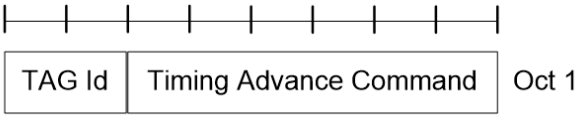


Figure 3.5 Timing advance command in a MAC Control Element (CE) message [9].

3.1.3 Time Alignment Timer

When a UE receives a TA command, it adjusts its uplink timing by TA seconds. The MAC entity (of the UE) has a configurable timeAlignmentTimer which it starts/restarts once it has applied the TA value. The timeAlignmentTimer is used to control how long the MAC entity is time aligned [9]. When this timer runs out, the MAC entity is no longer considered time aligned.

Upon receiving a TA command, the MAC entity must do the following [9]:

1. Upon receiving a TA command in a MAC control element message, i.e., a TA type 2:
   - apply the TA command for the indicated Timing Advance Group (TAG).
   - start or restart the timeAlignmentTimer associated with the indicated TAG.
2. Upon receiving a TA command in a Random Access Response (RAR) message, i.e., a TA type 1:
   - if the Random Access Preamble was not selected by the MAC entity:
     - apply the TA command for this TAG.
     - start or restart the timeAlignmentTimer associated with this TAG.
   - else, if the timeAlignmentTimer associated with this TAG is not running:
     - apply the TA command for this TAG.
     - start the timeAlignmentTimer associated with this TAG.
3. When the timeAlignmentTimer expires:

- if the timeAlignmentTimer is associated with the primary Timing Advance Group (pTAG):
  - flush all HARQ buffers for all serving cells.
  - notify Radio Resource Control (RRC) to release PUCCH for all serving cells.
  - notify RRC to release SRS for all serving cells.
  - consider all running timeAlignmentTimers as expired.
- else if the timeAlignmentTimer is associated with a secondary Timing Advance Group (sTAG), then for all serving cells belonging to this TAG:
  - flush all HARQ buffers.
  - notify RRC to release SRS.
  - notify RRC to release PUCCH, if configured.

3.2 EXPLORING TIMING ADVANCE FOR NAVIGATION

The aim of this section is to explore Timing Advance for localisation. It will begin by discussing the hardware required to get GPS and cellular data, followed by the software which will run on the hardware, the experimental setup, and finally the results.

3.2.1 The Cellular and GPS Module

The COTS Ublox EVK-R280 Evaluation Kit contains an on-board GNSS module and a cellular module. The cellular module is the Ublox LARA-R280 and the GNSS module the Ublox NEO-M8N. Figure 3.6 shows the specifications of the EVK-R280, i.e., the LTE/UMTS RF frequencies it supports, its communication interfaces, positioning capabilities, etc. Figure 3.7 shows the block diagram of the EVK-R280, which includes both the GNSS and cellular modules and how they are interconnected.

Model	Region	Radio Access Technology			Positioning			Interfaces						Audio		Features										Grade		
		LTE bands[1]	UMTS bands	GSM bands	GNSS via modem	AssistNow Software	CellLocate®	UART	USB 2.0	HSIC *	SDIO *	DDC (I²C)	GPIOs	Analog audio	Digital audio	Network indication	VoLTE	Antenna supervisor	Rx Diversity	Jamming detection	Embedded TCP/UDP stack	Embedded HTTP,FTP,SSL	FOTA	eCall / ERA GLONASS	Dual stack IPv4/IPv6	Standard	Professional	Automotive
LARA-R280	APAC	3,8,28	2100		●	●	●	1	1	1	1	1	9		●	●	■	●	●	□	●	●	●		●		■	

● = Available in any firmware ■ = CSFB only □ = Available in future firmware * = HW ready

Figure 3.6 Ublox EVK-R280 specifications [45].

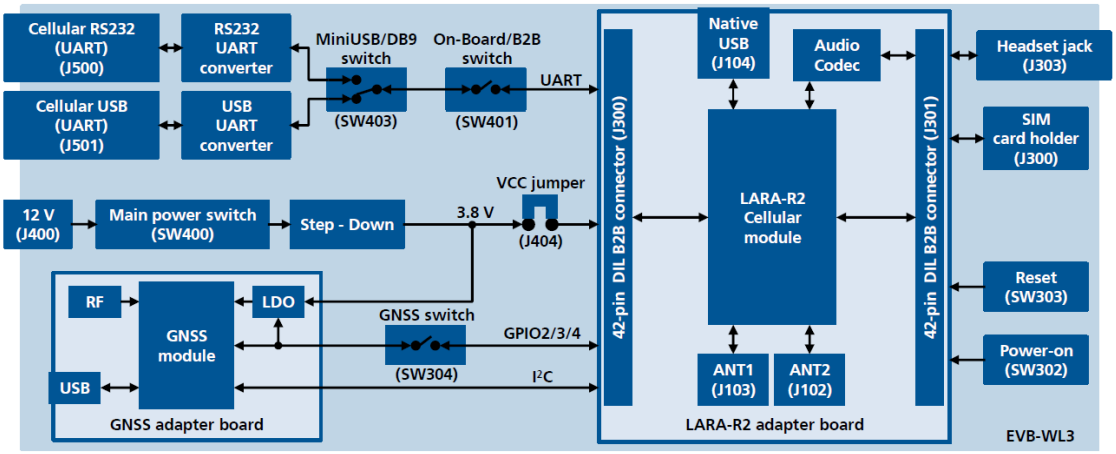


Figure 3.7 EVK-R280 block diagram showing an on-board GNSS module, cellular module, SIM card holder, power port, and its communication interfaces [44].

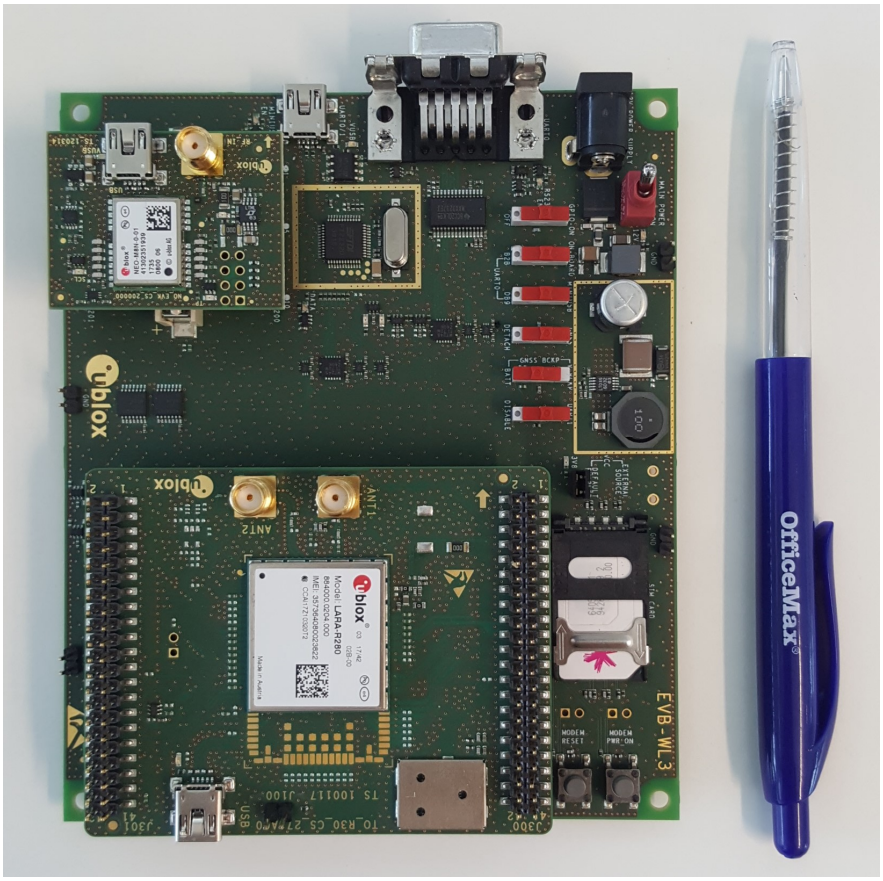


Figure 3.8 The EVK-R280 Evaluation Kit placed next to a pen for size comparison.

3.2.2 The Software: Communicating with the EVK-R2

In order to set-up/communicate with the LARA-R280 and GNSS modules the vendor supplied software 'm-center' was used. m-center also provides a terminal for sending AT[1] commands which can be used to request both cellular and GNSS data. It is available for downloaded from the Ublox website.[2] Figure 3.9 shows m-center's GUI and Figure 3.10 its terminal program. Instructions on how to connect the LARA-R280 to m-center is provided in Appendix A.

[1] AT commands are a set of commands that are used to interface with a modem. The Ublox AT command set is available at `https://www.u-blox.com/sites/default/files/u-blox-CEL_ATCommands_%28UBX-13002752%29.pdf`.

[2] `https://www.u-blox.com/en/product/m-center`

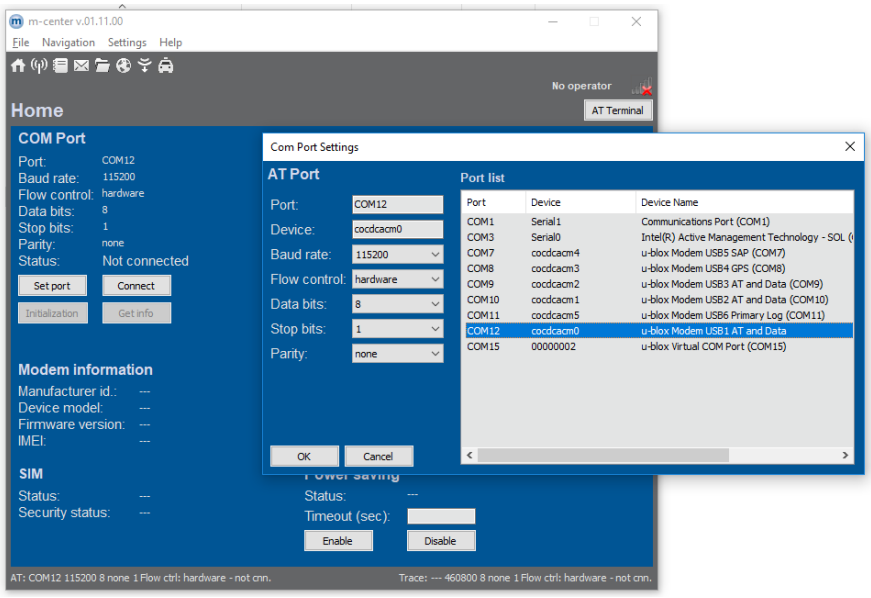


Figure 3.9 The m-center GUI; used to select a serial port, set port settings, and connect to the LARA-R280.

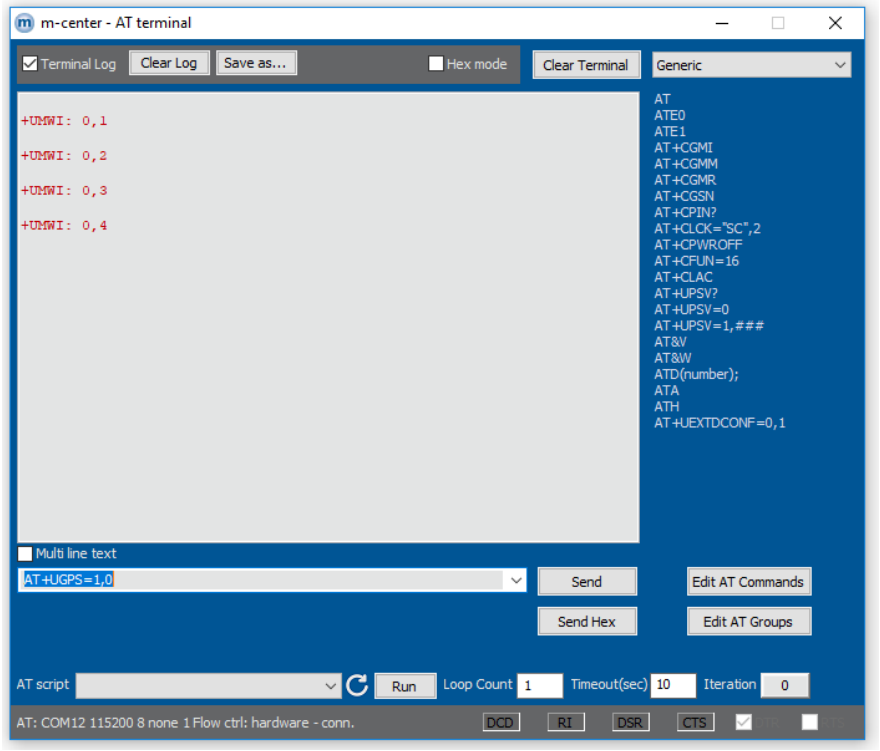


Figure 3.10 The m-center terminal; used to configure and communicate with the LARA-R280 via AT commands.

All AT commands typed into m-center's terminal and its responses are automatically stored into a log file ('.log' extension) which is stored on disk. AT scripts ('.atl' extension) can be written to automate processes. An AT script is a list of AT commands, which

can be imported into the terminal and executed. A “loop count” value between 1 and 1000 can be selected to repeatedly run the script.

3.2.2.1 AT Scripts

Three AT scripts were written in order to set up the LARA-R280 to obtain data during field tests. A screenshot of each script is shown in Figure 3.11, 3.12, and 3.13. m-center does not have a text editor for editing scripts, but an external text editor can be used.

The initialisation script (see Figure 3.11) initialises the EVK-R2; i.e., enabling verbose error results codes, unsolicited result codes (URCs), turning on the GNSS module, storing the most recent NMEA[3] sentences of interest, and network registration.

```
AT+CMEE=2       //n=2: <err> result code enabled and verbose <err> values used.
AT+CREG=2       //n=2: network registration & location info URC <stat>[,<lac>,<ci>[,AcTStatus>]] enabled
AT+UGPS=1,1     //turn GNSS module on with local aiding
AT+UGIND=1      //enable GNSS URCs
AT+CMGF=1       //Indicates the format of messages used with send, list, read and write commands and URCs
                //resulting from receiving SMSes messages (1= text mode)

AT+CSDH=1       //Controls whether detailed SMS header information is shown in text mode (1: show detailed
                //SMS header information)

AT+CGSMS=2      //Specifies the service (PS or CS) or service preference that the MT will use to send
                //mobile originated (MO) SMS messages. 2: PS preferred (use CS if PS is not available)

AT+UGGLL=1      //Enables the storing of the last value of NMEA $GPGLL messages
AT+COPS = 2     //de-regiser from the network (needed to carry out next instruction.)
AT+URAT=3,3     //(3,3) = (selectedAct, PreferredAct) = (LTE(single mode), LTE)
                //(6,3) = (selectedAct, PreferredAct) = (UMTS/LTE dual mode, LTE) <== default

AT+COPS=0       //re-register to the network. (0 = automatically)
```

Figure 3.11 Initialisation AT script; the commands shown are used to initialise the device, i.e., turn on the GNSS module, etc.

The second script (see Figure 3.12) was used to set up a Packet Switched Data (PSD) connection in order to ping an external IP address, through DNS lookup, of a known URL such as www.google.com. The ping command transmits uplink data which the network can use to measure the TA value.

[3]NMEA (i.e., NMEA 0183) is a combined electrical and data specification for communication between marine electronics, e.g., GPS receivers. A “NMEA sentence” refers to a sentence of GPS data including, for example, a GPS fix.

```
AT+UPSD=3,0,0                        //choose IPv4 as protocol type for PSD profile 3
AT+UPSD=3,1,"www.vodafone.net.nz"    //set "www.vodafone.net.nz" as APN
AT+UPSD=3,4,"8.8.8.8"                //set primary DNS
AT+UPSD=3,5,"8.8.4.4"                //set secondary DNS
AT+UPSD=3,100,3                      //map PSD profile 3 to context id (cid) 3
AT+UPSDA=3,3                         //activate PDP context specified in PSD profile 3
AT+CGDCONT?                          //return defined connection params for PDP context
AT+UPING="www.google.com"            //ping www.google.com
AT+UPSND=3,0                         //return IP address assigned to PSD profile 3
AT+UPSND=3,8                         //check PSD profile status (1=active)
AT+CGATT?                            //check gprs attachment state (1=attached)
AT+CGACT?                            //show state of PDP context (1=activated)
AT+CGPADDR=                          //show PDP address for all context ids (cid)
AT+CGREG=2                           //enable network reg. & location info URC
AT+UREG=1                            //network reg. attach status URC +UREG enabled
AT+CGCONTRDP=1                       //return some info about PDP context 1
AT+CGCONTRDP=3                       //return some info about PDP context 3
```

Figure 3.12 An AT script containing the AT commands required to set up a Packet Switched Data (PSD) connection. Once a PSD connection is established, uplink data (via pings) can be sent to the eNB so that it can measure the TA value.

The positioning script (see Figure 3.13) is used to obtain data for positioning. It continually sends the following four AT commands to the EVK-R2:

1. The ping (UPING) command which transmits data uplink for the network to measure the TA value.

2. The UGGLL command which retrieves the most recent NMEA $GPGLL sentence containing the UE's latitude, longitude, and time of fix; to be used as ground truth.

3. The CESQ command which gets the Received Signal Received Power (RSRP), and the Received Signal Received Quality (RSRQ).

4. The CGED command which gets the TA value, TA type, cell ID, radio access technology (RAT), as well as the mobile country code (MCC) and mobile network code (MNC) which are used to determine what network the UE is connected to. A snapshot of a CGED command's response is presented in Figure 3.14.

```
AT+UPING="www.google.com"   //ping google.com so that data is constantly sent to the
                            //network and thus TA value is measured and sent back
AT+UGGLL?                   //get $GPGLL value (i.e. lat and lon)
AT+CESQ                     //extended signal quality (gets RSRP & RSRQ if using LTE)
AT+CGED=4,0                 //get cellid and TA. (4,0) = (mode, details)

Supported modes:
• 0 (default value): one shot dump
• 1: periodic refreshed dump; information for up to 32 neighbour cells is available
• 2: stop periodic dump
• 3: one shot serving cell dump
>> • 4: periodic serving cell refreshed dump
Test the following 2 options and see if results are returned more frequently
>> • 128: one shot dump without the tags
>> • 129: periodic refreshed dump without the tags
• 131: one shot serving cell without the tags
• 132: periodic serving cell refreshed without the tags
```

Figure 3.13 Positioning AT script; contains the commands used to obtain cellular data from the cellular module and GPS data (for ground truth) from the GNSS module.

```
[14:27:42.483] tx: +UGGLL: 1,$GPGLL,4331.31269,S,17234.82330,E,012742.00,A,A*75
[14:27:47.992] tx: +CGED: RAT:"LTE",
[14:27:47.992] tx: MCC:530, MNC:05, CellID:271491, PhyCellId:176, TAC:28161, RSRP:81, RSRQ:27, TA:0, TA_type:2
```

Figure 3.14 The response of 1) the +UGGLL command (blue) containing lat, lon, and GPS time of fix, and the response of 2) the +CGED command which contains the TA value, TA type, cell ID, etc.

Limitation of the LARA-R280:

Because the LARA-R280 module was not designed for positioning, which was also the case for all other COTS cellular modules researched in this project, it has many limitations which make positioning with it difficult. E.g., the following:

- The module can only get TA values from the eNB it is connected to. Researchers in [28], using a GSM modem for positioning, were able to get TA values from up to six neighbour cells as well as the serving cell.
- TA values can only be obtained if the UE has an internet connection, so that it can transmit uplink data to the network to measure the TA value.
- TA values can only be obtained from the host network. E.g., when connected to the Spark network, the UE is only able to get TA values from Spark eNBs. In New Zealand, this means being able to utilise less than half of all eNBs.

3.2.2.2 Database of Cell Tower Locations

In order to obtain GPS pseudoranges, i.e, the distance between a UE and eNB to be used as ground truth, the location of all eNBs that the UE will connect to must be known. This data is available on Radio Spectrum Management's (RSM) Register of Radio Frequencies[4], but obtaining this data is challenging as the data is scattered across multiple web pages.

An easier solution is to obtain this data from GIS Geek[5]; a website which uses the Google Maps API to plot the location of all cell towers in New Zealand. It takes its data from RSM's Register of Radio Frequencies and stores them in a tabulated format in a Google Fusion Table; as shown in Figure 3.15. A CSV version of this data was downloaded to disk for use in the Python scripts of the following sections.

[4] https://www.rsm.govt.nz/smart-web/smart/page/-smart/WelcomePage.wdk
[5] https://gis.geek.nz/celltowers

gisg_cellsites

Attribution unknown - Edited on 2018 June 12

File Edit Tools Help | Rows 1 | Map 1 | Cards 1 +

Filter No filters applied

1-100 of 5090

id	easting	northing	client	bands	gmap_marker
25	175.714000000	-36.852900000	Spark	|850|1800|700|2300|	blu_diamond
52	176.886000000	-39.496900000	Vodafone	|2100|900|1800|	red_diamond
76	174.828000000	-36.892500000	2Degrees	|900|2100|1800|	grn_diamond
83	174.767000000	-36.844000000	2Degrees	|2100|	small_green
577	174.285000000	-39.590800000	Spark	|2100|	small_blue
747	178.359000000	-37.806600000	Vodafone	|900|	small_red

Figure 3.15 Cell tower data (coordinates, tower ID, network, etc.) from GIS Geek stored in a Google Fusion Table.

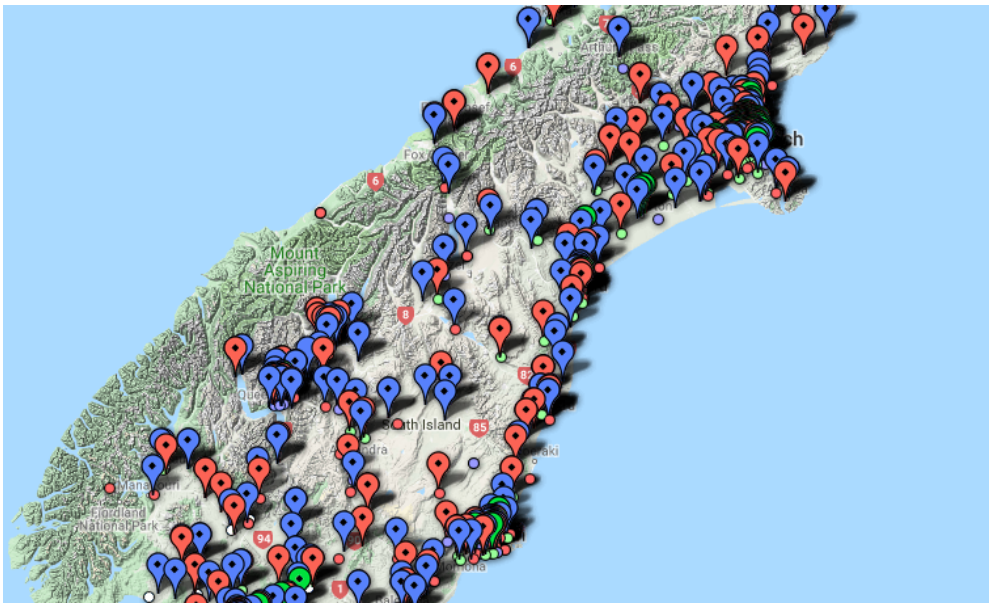


Figure 3.16 Screenshot from GIS Geek showing the cell towers of the lower South Island, in New Zealand.

3.2.3 Experimental Setup

Figure 3.17 shows the block diagram of the system that was used for data collection. The GNSS module was used to get the location of the UE for ground truth, and the cellular module was used to get TA data. The GNSS antenna was placed on top of the vehicle's dashboard under the windscreen of the vehicle. One LTE antenna was attached near the top-centre of the windscreen, and the other on the top-centre of the

front passenger window. TA and GPS data was recorded during a trip which involved driving a large loop in Christchurch city, New Zealand.

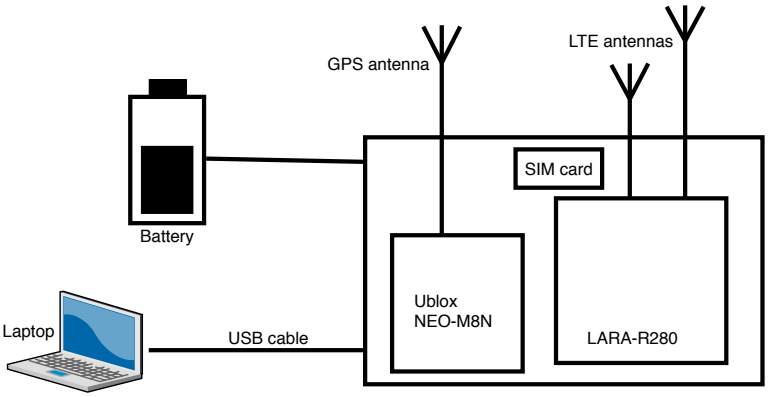


Figure 3.17 Block diagram of the system used for data collection. It includes 16.8 V (at full charge) 4S LIPO battery, a laptop, and the Ublox EVK-R2 development kit which contains the Ublox NEO-M8N GNSS module, SIM card holder, and LARA-R280 cellular module. The GNSS antenna is a 3.3 V active patch antenna, and the two LTE antennas are 700–2800 MHz I-Bar antennas.

3.2.4 Data Processing

The aim of this section is to determine how accurate TA pseudoranges are compared to GPS pseudoranges. The granularity of a TA value is ∼78 m, hence, the aim is to get as close to this as possible. Ideally, the GPS pseudoranges, i.e., the distance between the UE and eNB (calculated using the Vincenty[6] formula from the Python GeoPy library) will fall within a band 78 m wide; the centre of the band to the eNB defined as the TA pseudorange, d_{TA}, calculated via the equation:

$$d_{\mathrm{TA}} = \mathrm{TA} \times 78.125 + 39.0625\,. \tag{3.5}$$

The width of this band is the granularity of the TA value; as depicted in Figure 3.18.

[6] `https://geopy.readthedocs.io/en/stable/#geopy.distance.vincenty`

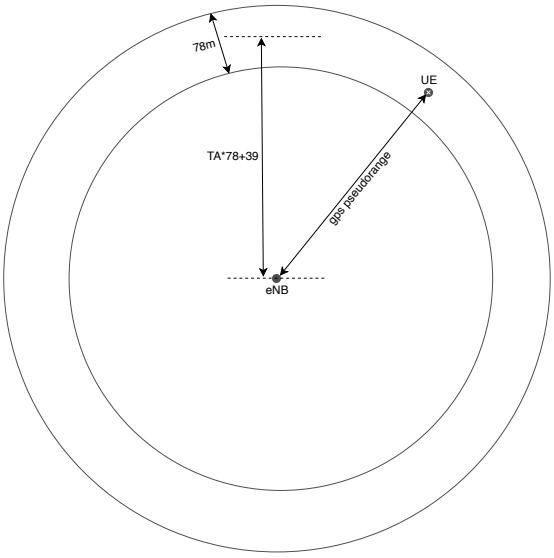


Figure 3.18 TA pseudorange vs. GPS pseudorange: The granularity of timing advance is 78 m (width of the band); ideally, GPS pseudoranges should always fall within this band.

The error, e, is the distance between the GPS pseudorange, d_{GPS}, and the TA pseudorange. That is:

$$e = d_{\mathrm{GPS}} - d_{\mathrm{TA}}\,. \tag{3.6}$$

If the TA pseudoranges and GPS pseudoranges are accurate then the errors should always fall within ± 39 m, i.e., within a 78 m wide band.

3.2.4.1 Scripts for Interpreting Log File Data

This section discusses the python scripts used to process and analyse the cellular data collected during field tests. The three scripts are named as follows:

1. process_raw_data.py
2. get_gps_and_TA_dist.py
3. gps_vs_TA_dist_graphs.py

Script 1, *process_raw_data.py*, traverses through a log file (i.e., raw field test data) and searches for sentences containing the results of the +CGED and +UGGLL commands. The +CGED results are parsed to get the TA value, TA type, cell ID, MCC, MNC, RSRP, RSRQ, and its time of fix (TOF). The +UGGLL results are parsed to get GPS latitude, longitude, and its time of fix. A snippet of this scripts CSV output is shown in Figure 3.19.

From	TOF	Lat	Lon	Cellid	TA_val	TA_type	RSRP	RSRQ	Speed
cellular	59:12.9	-43.5458	172.5049	272507	5	1	69	26	58.33173
cellular	59:18.2	-43.5459	172.5039	272507	5	1	67	24	60.22018
cellular	59:23.4	-43.5459	172.5028	272507	5	1	72	27	65.19519
cellular	59:28.6	-43.546	172.5016	272507	5	1	66	29	67.36044
cellular	59:33.9	-43.5461	172.5003	272507	5	1	65	24	67.01403
cellular	59:39.2	-43.5464	172.4992	272507	5	1	58	19	66.85064
cellular	59:44.5	-43.5468	172.4981	272507	5	1	60	19	67.2706

Figure 3.19 A snippet of the CSV output of script one (process_raw_data.py).

Script 2, *get_gps_and_TA_dist.py*, operates on the CSV output of script one (process_raw_data.py). Using this information and a database containing the coordinates of all cell towers, it calculates TA distance, GPS pseudorange, and the error between the two. It also copies over other values such as RSRP, RSRQ, TOF, and UE speed. A snippet of this script's CSV output is shown in Figure 3.20.

cell_id	gps_dist	TA_dist	dist_error	rsrp	rsrq	TOF	speed
425329	1375.538	1445.313	-69.7747	64	25	59:54.8	63.11714905
425329	1292.398	1445.313	-152.915	62	21	00:00.0	62.64945425
425329	1210.35	1445.313	-234.963	63	23	00:05.2	59.11450872
425329	1103.524	1445.313	-341.788	61	24	00:10.4	64.64593155
425329	1013.444	1445.313	-431.868	70	26	00:15.7	65.01678253
425339	47.37264	39.0625	8.310144	77	26	01:12.5	74.61600314
425339	119.6973	39.0625	80.6348	66	26	01:17.9	76.28708751

Figure 3.20 A snippet of the CSV file containing the results of script two (get_gps_and_TA_dist.py).

Script 3, *gps_vs_TA_dist_graphs.py*, operates on the CSV output of script 2, plotting a series of graphs to analyse and understand the TA data. The following observations were made:

1. TA type 2s always have a value of 0, which mean A) neither advance or retard uplink transmissions, or B) they are false and should be ignored. Equation (3.7) is used to determine how much uplink transmissions should be advanced or retarded by.

$$N_{\text{TA,new}} = N_{\text{TA,old}} + (\text{TA} - 31) \times 16T_s\,. \tag{3.7}$$

This indicates that upon receiving a type 2 TA value of 0, the UE should retard its transmissions by 16.12 us; since $(0 - 31) \times 16T_s = -16.12\,\mu$s. The issue is that the UE only outputs TA = 0, when the UE is stationary or if it is moving but is not transmitting any uplink data. When the UE is stationary, TA type 2 values should be 31, since $(31 - 31) \times 16T_s = 0$, prompting the UE to make no changes to its uplink timing. In all the data obtained so far, all TA type 2s had a value of

zero. Hence, they were all ignored as they provided no useful information. The zero values are likely caused by incorrectly implemented reporting of type 2 TA values in the LARA-R280 firmware.

2. On average one TA value was obtained every 5.2 s (including both types).

3. If the UE was moving and transmitting uplink data, all obtained TA values were type 1s. Figure 3.21 shows that once a type 1 TA value was obtained, that same value would be provided for some time; i.e., 58 s on average (see Figure 3.22) before another (fresh) value was obtained. The repeated values are false, and hence, not useful for positioning.

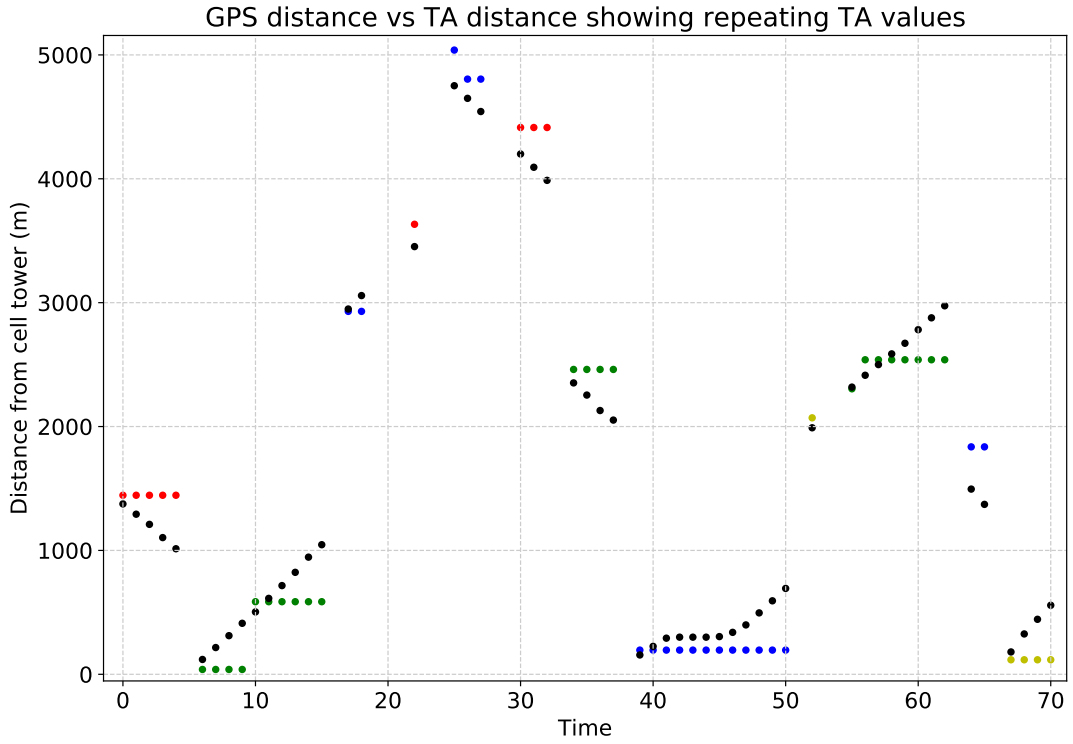


Figure 3.21 Plot of TA distances (coloured) alongside GPS pseudoranges (grey). It shows GPS pseudoranges changing from one sample to another (as it should since the UE is moving) but the TA values usually remains constant until handover, when the UE connects to another eNB and receives a new TA value (i.e., not a repeat). Each change in colour indicates a handover (i.e., connection to a new eNB).

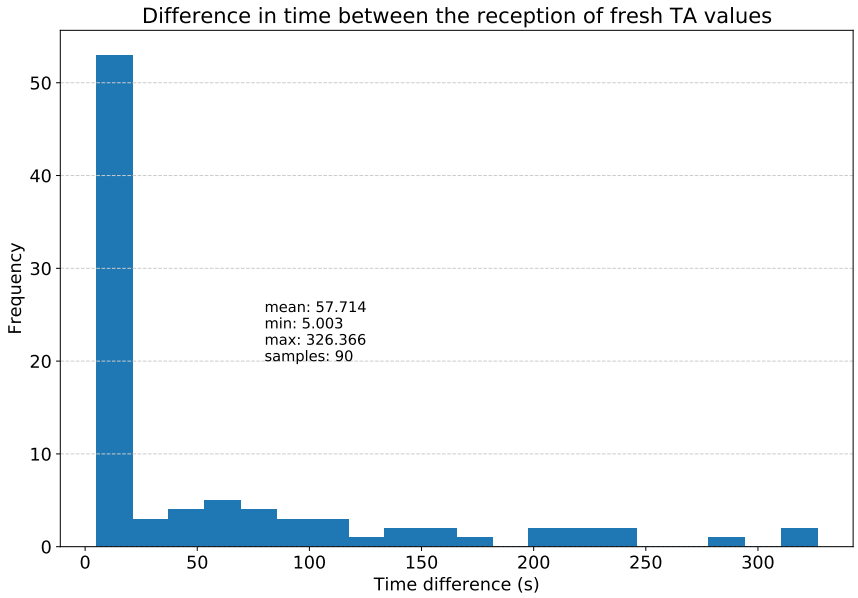


Figure 3.22 The plot shows the time difference between the reception of "fresh" TA values and excludes repeated values. On average a fresh TA value was obtained once every 58 s.

4. TA distances calculated from repeated TA values give false results. This is evident from Figure 3.21 where the initial TA distance (obtained from a fresh TA value) is relatively close to the GPS pseudorange, but subsequent TA distances diverge, until another fresh TA value is obtained.

5. Because the majority of TA values obtained are redundant, e.g., repeated type 1 TA values, the effective update rate of timing advance is one update per ∼58 s (see Figure 3.22).

All observations made so far are based on data collected from the Ublox LARA-R280 module while connected to the Spark and Vodafone networks. This does not provide enough information to conclude that these TA rates will be experienced by all other cellular modules on all networks.

When all the repeated type 1 TA values and type 2 TA values are ignored, the positioning results from the remaining (i.e., useful) type 1 TA values provide a clear correlation between GPS pseudoranges and TA distances (see Figure 3.23). Hence, Timing Advance can be used for positioning, but the accuracy is worse than expected. Ideally, the errors between TA distances and GPS pseudoranges should fall within a 78 m wide band. Instead, the errors lie within +50 and -250 metres (2σ), i.e., a 300 m wide band as shown in Figure 3.24. There's also a bias of -110 m.

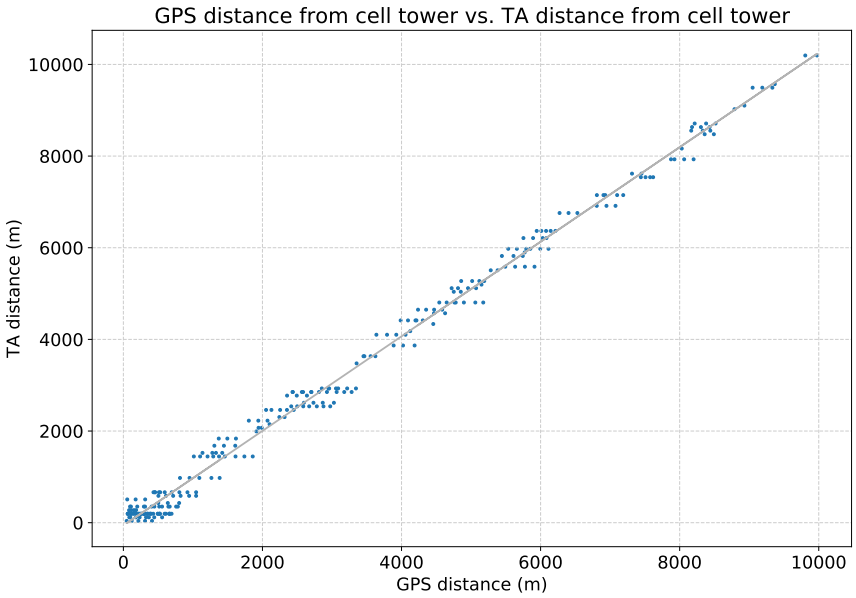


Figure 3.23 Scatter plot of TA pseudoranges vs. GPS pseudoranges. This graph is based on fresh TA values and excludes repeated values. It shows a clear correlation between the TA pseudoranges and GPS pseudoranges.

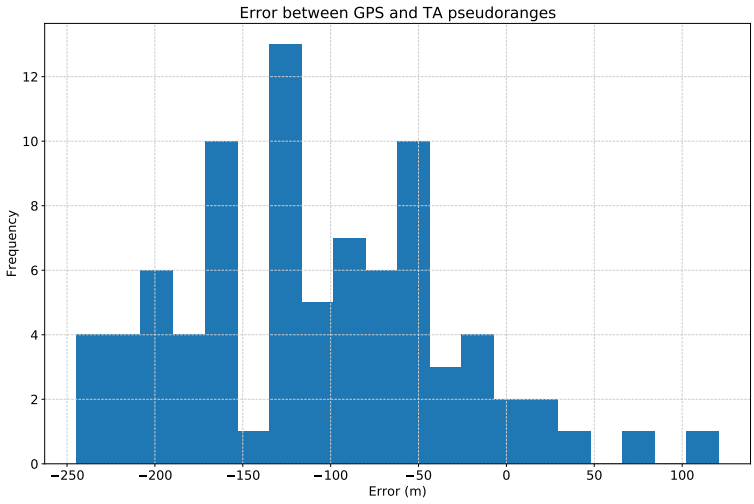


Figure 3.24 A histogram of the errors between TA and GPS pseudoranges. It is centred at -110 m.

The bias of -110 m was initially thought to be from the unaccounted cell tower height. TA pseudoranges calculated from TA values so far have assumed the TA pseudoranges (slant height) to be equal to the horizontal distance to the tower. From Figure 3.25 it is clear that the slant height is actually bigger and since the error is $d_{\text{GPS}} - d_{\text{TA}}$, a larger slant height would always result in a negative error which the bias is. But, the eNB antennas in Christchurch, New Zealand are not very high, and typically located at less than 30 m above ground level (AGL). Hence, the maximum error this can cause is the height of the tower which would occur if the UE is situated on the ground directly

under the eNB antennas. When the UE is 100 m from the cell tower the error would only be 5 m assuming the eNB antennas are at 30 m AGL. Usually the UE is much farther than this where the error is much less and practically negligible.

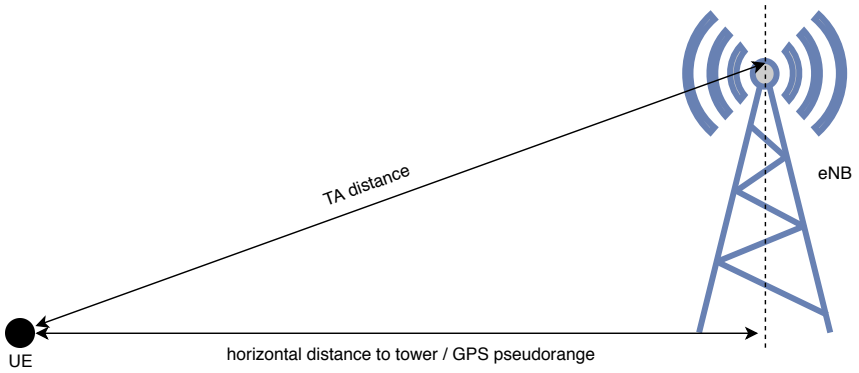


Figure 3.25 The TA pseudorange is the slant height between the EU and eNB antenna. So far it has been assumed to be equal to the horizontal distance which appears much shorter. For all practically purposes, the error caused by this discrepancy is negligible.

The mostly likely cause of the -110 m bias in the distance errors is multipath. If this is the case, the TA value will be the round-trip time of a signal that is not the LOS signal, hence, resulting in a larger value than the LOS value. The GPS pseudorange between the eNB and UE is the straight-line distance. Since the error is calculated as $e = d_{\text{GPS}} - d_{\text{TA}}$, a larger TA distance will result in a negative error value. Since the UE was situated on a ground vehicle, and surrounded by many structures such as trees and houses, multipath is very likely.

A possible cause for the large errors of 300 m, instead of the expected 78 m is likely the following:

1. **The time delay between GPS fix and TA value (see Figure 3.26):**
   The +CGED command (a.k.a TA command) obtains ∼10 different parameters including the TA value.[7] The order of parameters and the amount of time each take to obtain is unknown. TA commands are issued periodically as shown in Figure 3.26. Each block represents the execution time of a single TA command. A command is issued at the beginning of a block, and its response is received at the end. Some time within this block the TA value is obtained, but, it is provided to the user at the end of the block. The GPS fix is also obtained at this time. Hence there is likely a time discrepancy between the actual time the TA value is obtained and the time the GPS fix is obtained; resulting in an error being added to the GPS pseudorange (ground truth). The error in distance is equal to the UE velocity times the time error.

[7]Parameters obtained include: MCC, MNC, Cell ID, Physical Cell ID, TAC, RSRP, RSRQ, TA value, TA type

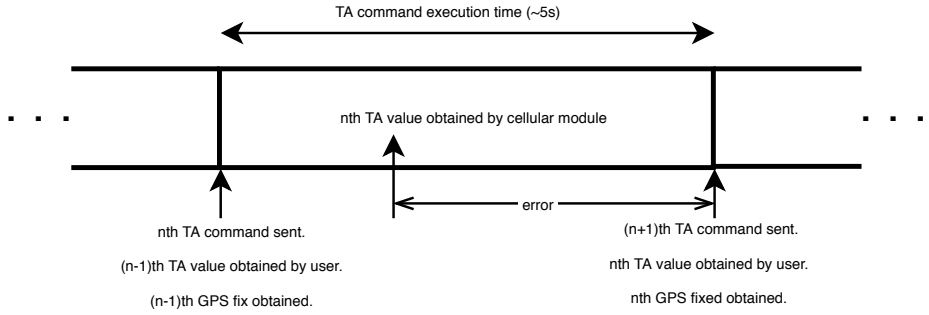


Figure 3.26 This diagram shows that the TA value and the GPS fix are not received at the same time. This resulting in an error being added to the GPS pseudorange (ground truth) that is equal to UE velocity times the time error. Since the time error is indeterminable, it is difficult to remove. This error is also likely to be variable.

2. **Multipath:**
   The large variance of 300 m in the errors between the GPS and TA distances is likely to be caused by multipath also. When the TA value is experiencing severe multipath the error between GPS and TA distances will be large; i.e, on the order of -250 m or more. When the TA value is not affected by multipath, the errors will be small and mainly from the quantisation (i.e., granularity) of the TA value. Hence, resulting in a wide variance.

3.3 IMPROVING TIMING ADVANCE UPDATE RATE WITH PYSERIAL

In the previous section the update rate of TA pseudoranges was found to be ∼58 seconds. This is rather infrequent and hence undesirable.

This section will discuss the use of PySerial to directly communicate with the Ublox cellular module. By using PySerial it is be possible to wait until a command's response is fully retrieved before issuing the next command ensuring that no data (esp. TA values) provided by the cellular module are lost.

The current hypothesis is that responses containing useful TA values are being discarded by m-center, in order to serve the next command. In m-center the wait time for the response of commands is unspecified. Different commands take variable amounts of time to execute and variable amounts of time to provide a response. The +CGED command, in particular, takes several seconds to execute and provide a response as it has to obtain many other parameters alongside the TA value. The execution time of the command also varies with each instance. Hence, it is plausible that the next command is occasionally issued before the command's response is fully received.

This is likely due to the limited functionality of m-center, i.e., it does not provide any means of waiting for a command's response to be fully received before sending the next command. As a result some TA values are likely discarded because the command timing out.

If this is the case, and TA values were being lost when using m-center, then using PySerial[8] these lost TA values should be captured, hence, increasing the update rate.

3.3.1 The PySerial Code

The PySerial code is split into two parts:

1. The first first part of the script is used to configure the LARA module, this includes turning on the GNSS module, setting up a PSD connection, enabling the buffering of wanted GNSS responses (e.g., GPGLL), etc. This is done by sending the exact AT commands that were sent to the module in the previous section, but from python code instead of an AT script.

2. The second part of the script is used to obtain positioning data and GPS fixes for ground truth. This part of the code contains an infinite loop that repeatedly sends the following commands and reads their responses:

   (a) Ping AT command which pings www.google.com. This sends uplink data to the network so that the TA value can be measured.

[8]PySerial is a python module that encapsulates the access for the serial port by providing the backend. The library is available at: `https://pyserial.readthedocs.io/en/latest/index.html`

(b) CGED AT command which provides the user the TA value.

(c) GPGLL AT command which provides the user the GPS fix of the module.

The full Python script is available in Appendix B.

3.3.2 Results

The results obtained show that the hypothesis was indeed correct, i.e., TA values were being discarded by m-center. Whether TA type 1s were being discarded or not by m-center is unknown, but, where virtually no non-zero (i.e., useful) TA types 2s were being received by m-center, there is a significant amount being received by PySerial.

In the latest trial, over a field test time of 15.5 minutes, there was approximately 178 TA values received; one every 5.2 s. The number of TA type 1s received was 21, and non-zero TA type 2s received was 32 — which averages to ∼18 s/update; a 3+ fold improvement over the previous update rate of ∼58 s.

The reason for the increased update rate is that when using PySerial, a significant a amount of non-zero (i.e. useful) TA type 2s were being obtained. On average 1.5 times more than the number of TA type 1s. Whereas, when m-center was being used to communicate to the cellular module, almost no non-zero TA type 2s were obtained. From ∼10 hours of total field testing a total of 5 non-zero TA type 2 values were obtained from m-center.

3.4 CONCLUSIONS

In the background section (Section 3.1) of Timing Advance, the theoretical accuracy of TA was stated as 78 m. Practical experiments using COTS equipment, i.e., the LARA-R280, resulted in a practical accuracy of 300 m (2σ). One reason for the cause of such large errors may be that the time-of-arrival of TA values are not synchronous with the timestamp of the corresponding GPS fixes; as described in Figure 3.26. The level of multipath, which depends on the environment, can also cause the distance errors to have a larger variance. The errors were also centred around -108 m, instead of 0 m, which is likely caused by multipath also.

A possible solution to reduce the size of the errors may be to use a Software Defined Radio[9] (SDR) implementation of the UE. In a SDR implementation it would be possible to obtain a TA value as soon as it arrives. If at the same instant the GPS fix is also obtained, there would be little time discrepancy between the timestamp of the TA value and GPS fix; hence, removing any errors caused by this discrepancy.

In the initial experiments, where TA data was obtained using Ublox's m-center interface, the update rate of TA pseudoranges was ∼58 seconds. When the same experiments were carried out using the PySerial interface to communicate to the cellular module an improved update rate of ∼18 seconds was obtained. The reason for this was the m-centre was discarding all non-zero valued type 2 TA values, hence, reducing the total number of useful TA values. Although a 3+ fold increase compared to the initial update rate, 18 s/update is still infrequent and likely to be insufficient for a practical positioning system. Hence, a method of improving this in needed.

[9]Software Defined Radios are discussed in Chapter 4 (next chapter).

Chapter 4

POSITIONING WITH LTE SIGNALS OF OPPORTUNITIES

4.1 BACKGROUND

This section explains how the Time-Of-Arrival (TOA) of LTE pilot sequences can be used to determine the distance between a UE and eNB, and hence, localise the UE. In the context of positioning these pilot sequences are often called signals of opportunities (SOP), since these signals are not designed for positioning, but they are opportunistically being exploited for that purpose.

The following section (4.1.1), which will explain the details, will assume the use of a LTE pilot sequence known as the SSS[1] (described in Section 4.5.2). The sequence is periodically transmitted by the LTE network; i.e., once every 5 ms.

4.1.1 How to use LTE Pilot Sequences for Localisation

Considering that the SSS is transmitted exactly once every 5 ms, when the UE is stationary, from the TOA of an initial SSS each subsequent SSS TOA will be some integer multiple of 5 ms. Hence, if the TOA of the initial SSS is t_0 and the TOA of the current SSS is t_n, then $(t_n - t_0) \bmod 5 \times 10^{-3} = 0$ seconds; where 0 is the remainder of the division and it is proportional to the distance the UE has moved towards/away from the eNB.

If the UE starts to move away from the eNB, while it is moving, each new SSS TOA will arrive slightly more than 5 ms apart from one another. Hence, if the current SSS TOA is t_n, then $(t_n - t_0) \bmod 5 \times 10^{-3} = \Delta t$, where the remainder of the division, Δt, is no longer 0, but greater than 0. The size of Δt depends on the speed of the UE and the amount of time it spent moving away from the UE; the faster the speed and the longer the period of movement the greater the value. By multiplying Δt by c (the speed of light in a vacuum), the distance, d, moved by the EU away from the eNB can

[1] SSS: Secondary Synchronisation Sequence

be obtained. That is,

$$d = \Delta t \times c\,. \tag{4.1}$$

The exact opposite happens when the UE is moving towards the eNB, i.e., the SSS TOAs will arrive slightly less than 5 ms apart from one another.

The following scenario will explain how the arrival of these pilot sequences can be used to localise the UE: A UE equipped with a GNSS receiver is situated on a UAV that is flying. During the flight, the UE's GNSS receiver is locked to GNSS, but, at time t_0 the GNSS lock is lost. The UE's last known position at t_0 is $\mathbf{r}_u = [x_u, y_u, z_u]$. During its flight the UE is also tracking/receiving pilot sequences from an eNB, whose location (known) is $\mathbf{r}_b = [x_b, y_b, z_b]$.

Hence, at time t_0, the straight-line distance, d_0, between the UE and eNB can be calculated using

$$d_0 = \|\mathbf{r}_u - \mathbf{r}_b\| = \sqrt{(x_u - x_b)^2 + (y_u - y_b)^2 + (z_u - z_b)^2}\,. \tag{4.2}$$

Assuming the signals travelling from the eNB to the UE are line of sight (LOS) signals, the time of flight of the signals, TOF_0, at t_0, would be

$$\mathrm{TOF}_0 = \frac{d_0}{c}\,. \tag{4.3}$$

AT t_0, when the UE was d_0 metres away from the eNB it received an LTE pilot sequence, whose time-of-arrival (TOA) was time-stamped as TOA_0. Hence, the time-of-transmit (TOT) of this sequence from the eNB must be

$$\mathrm{TOT}_0 = \mathrm{TOA}_0 - \mathrm{TOF}_0\,. \tag{4.4}$$

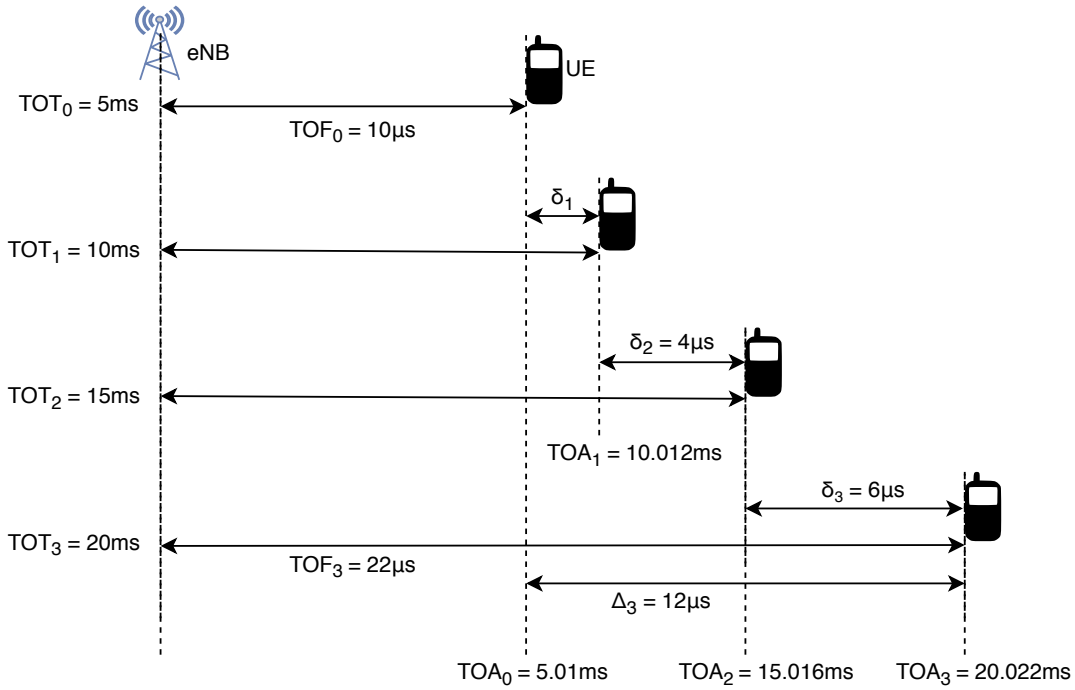


Figure 4.1 This diagram shows how LTE TOAs can be used to estimate the distance between a UE and eNB. If the time-of-arrival of a LTE pilot sequence is measured to be TOA_0, and at this time the distance between the UE and eNB is d_0 (determined from GNSS), then the time-of-transmit of the sequence that arrived at TOA_0 is determined as $\mathrm{TOT}_0 = \mathrm{TOA}_0 - \mathrm{TOF} \times c$. From this, the transmission times of all subsequent sequences are also known; they will be transmitted at some multiple of 5 ms from TOT_0; as shown on the left side of the diagram. Since the TOA of these transmitted sequences are measured they are also known. With this knowledge, the distance between the UE and eNB can be determined at a later time when GNSS is unavailable, i.e., at TOA_3. Knowing that the the pilot sequence arriving at TOA_3 was transmitted at TOT_3, the TOF of the this signal can be calculated as $\mathrm{TOF}_3 = \mathrm{TOA}_3 - \mathrm{TOT}_3$; multiplying this result by the speed of light, c, gives the distance between UE and eNB at time $t = \mathrm{TOA}_3$.

Once TOT_0 is known, then the the distance between the UE and eNB can be determined at all subsequent times as long as the UE continues to track the pilot sequence. As shown in Figure 4.1, once TOT_0 is known, all subsequent TOTs will also be known; they will be transmitted at exact multiples of 5 ms from TOT_0. The TOAs mark the arrival of the transmitted sequences at the UE. Since they are monitored and time-stamped, they are also known. Hence, the TOF of all subsequent sequences can be determined. E.g., at TOA_3, when GNSS is unavailable, $\mathrm{TOF}_3 = \mathrm{TOA}_3 - \mathrm{TOT}_3$. Hence, the distance between the UE and eNB, at $t = \mathrm{TOA}_3$ is $d_3 = c \times \mathrm{TOF}_3$.

A simpler way of getting the distance, d_3, between UE and eNB, with reference to Figure 4.1, is as follows:

$$d_3 = c \times \mathrm{TOF}_3\,, \tag{4.5}$$

where

$$\begin{aligned} \mathrm{TOF}_3 &= \Delta_3 + \mathrm{TOF}_0 && (4.6)\\ &= 12\mu s + 10\mu s && (4.7)\\ &= 22\mu s && (4.8) \end{aligned}$$

and

$$\begin{aligned} \Delta_3 &= (\mathrm{TOA}_3 - \mathrm{TOA}_0) \bmod 5 \times 10^{-3} && (4.9)\\ &= (20.022 - 5.01) \bmod 5 && (4.10)\\ &= 0.012\, ms = 12\mu s && (4.11) \end{aligned}$$

$\Delta_3 \times c$ is the distance that the UE has moved away from the eNB from TOA_0 to TOA_3. By adding TOF_0 to Δ_3 and multiplying the result by c the distance between the UE and eNB can be obtained.

Another method of determining Δ_3 is to use Equation 4.12, where

$$\Delta_3 = \delta_1 + \delta_2 + \delta_3\,. \tag{4.12}$$

While this method seems feasible it is not reliable, as Δ_3 will accumulate the quantisation[2] errors of every TOA from TOA_0 to TOA_3. Obtaining Δ_3 using Equation 4.9 is more reliable as it is only affected by the quantisation errors of TOA_0 and TOA_3.

In general, at the arrival of the n^{th} TOA, TOA_n, the distance between the UE and eNB, d_n, can be determined using the following equations:

$$\begin{aligned} d_n &= \mathrm{TOF}_n \times c && (4.13)\\ &= (\Delta_n + \mathrm{TOF}_0) \times c && (4.14)\\ &= \Delta_n \times c + d_0\,, && (4.15) \end{aligned}$$

where

$$\Delta_n = (\mathrm{TOA}_n - \mathrm{TOA}_0) \bmod 5 \times 10^{-3}\,. \tag{4.16}$$

By tracking pilot sequences from three different eNBs the UE can use circular trilateration to localise itself in the absence of GNSS signals, in 2-dimensions, as depicted in Figure 4.2. By tracking at least four eNBs, the UE can get a unique position fix in 3-dimensions.

[2]The quantisation size is equal to the sampling period T_s.

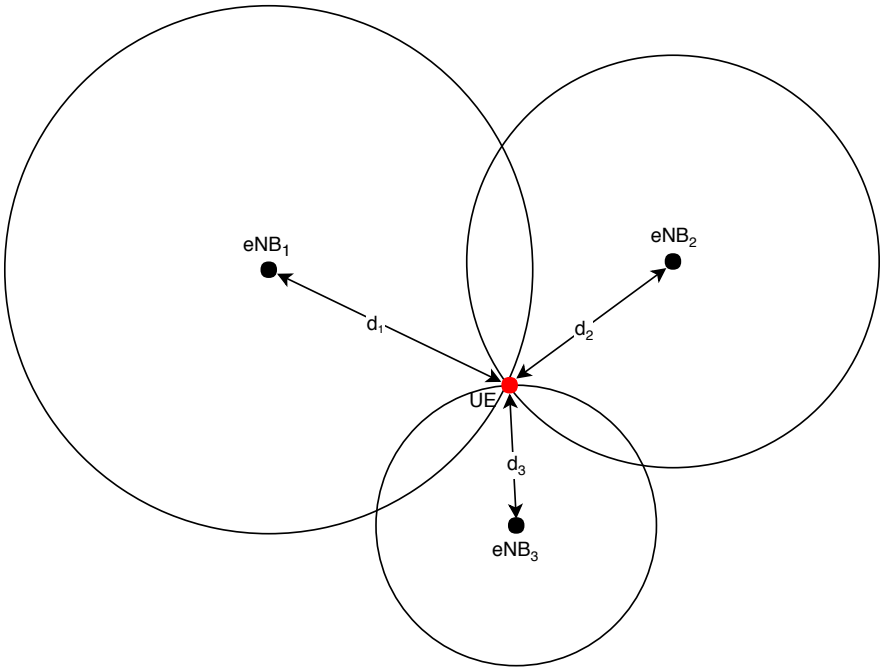


Figure 4.2 Circular trilateration using pseudoranges obtained from LTE eNBs.

NOTE: This method assumes that the location of all eNBs are known a priori. This data may be available publicly; for this project, all eNB locations were obtained from GIS Geek. Other ways of obtaining this data include ground surveys or satellite imagery.

4.1.2 Positioning Accuracy

Theoretically the positing accuracy of a system depends on the resolution of its timestamps. The sampling frequency, F_s, of srsLTE is 23.04 MHz, hence, its timestamp resolution will be $1/F_s = 43.4\,ns$. This equates to a positioning granularity and, hence, a best case theoretical positioning accuracy of 13 m.

It is possible to improve the resolution of TOAs by sampling at a higher frequency (oversampling). This will result in a higher data rate which in turn may require a more powerful SDR front-end and PC to be able to process the extra data.

Another option is to use the Francois Blais and Marc Rioux peak detector algorithm which uses an FIR filter and linear interpolator to increase the precision of the peak detection to better than one T_s [15] — instead of rounding the TOA to the nearest sample time.

4.1.3 Limitations

There are various other factors that will affect the accuracy of this method; such as:

- **Clock accuracy**
  Since positioning is highly dependent on accurate timing, if the time keeping

device (i.e., clock) has poor stability, then the TOAs obtained can have large errors resulting from both the drift of the clock and its jitter. Hence, the accuracy of positioning will be limited by the quality of the clock, and the algorithms used to estimate and compensate for timing errors.

- **Base station location accuracy**
  Base station coordinates obtained from GIS Geek may have errors up to $\sim$30 m. To obtain better position accuracy, tower locations must be determined more accurately. More accurate tower coordinates can be obtained via ground surveys.

- **Cell tower height**
  The cell tower locations obtained from GIS Geek only provide the horizontal (2D) coordinates of the cell towers. In order to do 3D positioning, the tower height is also required. This can be obtained at a later stage via ground surveys.

4.2 SOFTWARE DEFINED LTE USER EQUIPMENT

In order to use LTE TOAs for positioning an LTE UE is required in order to capture LTE pilot sequences. Chapter 3 showed that COTS LTE UEs have limited functionality, do not provide any means of accessing and modifying low level processes (e.g., relating to the pilot sequences), or any means of modifying the receiver to so that it can be used for positioning. The only other option is a software-defined LTE UE which is simple to modify since all of its processes are implemented in software and run on a general processor; hence, providing full customisability.

The three most well known software defined LTE UE are:

- **GNU Radio LTE Receiver (gr-lte)**
  gr-lte[3] is an open source software package which provides a GNU-Radio[4] based LTE receiver to receive, synchronise, and decode LTE signals. It is designed to be modular and uses GNU-Radio's processing blocks whenever available [29]. The advantage of this is that the blocks can be easily edited or replaced by other blocks to change or improve its functionality. Another advantage is that it is easy to track signals as they go from block to block, due to the modular structure provided by GNU Radio. Hence, making it quick and easy to understand, from a high level, how LTE works.

  The downside of this gr-lte is that it is not a complete implementation of an LTE receiver, missing a lot of the later stages of an LTE receiver. However, it does have the Cell Search and Synchronisation blocks which operate on the PSS and SSS pilot sequences. Hence, it should be possible to monitor these sequences and assess their feasibility for positioning.

  After a few weeks of working with gr-lte, although it made LTE simple to understand (due to the modular structure of the LTE receiver), the actual implementation of the blocks were difficult to understand and sometimes erroneous. Hence, using gr-lte for positioning turned out to be difficult and srsLTE was used instead.

- **openLTE**
  OpenLTE[5] is an open source implementation of the 3GPP LTE specifications focusing is on transmission and reception of the downlink signals [49]. While it implies that a receiver implementation is available, it was never found.

- **srsLTE**
  srsLTE is a free and open source LTE software suite developed by Software Radio Systems[6]. It is LTE Release 8 compliant (with selected features from

[3] `https://www.gnuradio.org/`

[4] GNU Radio is a free open-source software development toolkit that provides signal processing blocks to implement software radios.

[5] `https://sourceforge.net/p/openlte/wiki/Home/`

[6] `http://www.softwareradiosystems.com/`

release 9) and was released under the AGPLv3 license [40]. The software suite and installation instructions are available at Github[7] . It includes the following packages:

- srsUE: a complete SDR LTE UE application featuring all layers from PHY to IP.
- srsENB: a complete SDR LTE eNB application.
- srsEPC: a light-weight LTE core network implementation with MME, HSS and S/P-GW.
- a highly modular set of common libraries from PHY, MAC, RLC, PDCP, RRC, NAS, S1AP, and GW layers.

This project started using srsUE when it was clear that gr-lte could not be used. It was also the only option that guaranteed a working LTE UE.

NOTE: On 19 January 2019, in an email to the 'srslte-users' mailing list, SRS announced the release of srsLTE 18.12 which supports the latest 3GPP 15.2.2 release. This project does not use srsLTE 18.12, but instead, uses the older 18.09 version which was the only available option when this project started.

4.3 SOFTWARE DEFINED RADIO

A software defined radio is defined as a "Radio in which some or all of the physical layer functions are software defined" [23].

That is, system components that are traditionally implemented in hardware (e.g., modulators, demodulators, filters, mixers, amplifiers, detectors, etc.) are instead implemented in software, e.g., on General Purpose Processors (GPP), Field Programmable Gate Arrays (FPGA), Digital Signal Processors (DSP), programmable System on Chip (SoC), or other application specific programmable processors, or a combination of them. For example, it is not uncommon for computationally intensive processes to be implemented on FPGAs or DSPs and the remaining less intensive processes to be implemented on GPPs [23].

The advantage is that software defined processes are modifiable; enabling new features and capabilities to be added to existing radios at a later date without any hardware modifications [23]. The limitations of traditional hardware based radios is that modifications can only be made through physical intervention resulting in higher production costs, minimal flexibility in supporting multiple waveform standards. By contrast, software defined radio technology provides an efficient and comparatively inexpensive solution to this problem, allowing multimode, multi-band and/or multi-functional wireless devices that can be enhanced using software upgrades [23].

[7] `https://github.com/srsLTE/srsLTE`

With regards to this project, the system as a whole, i.e., the B200mini front-end and the PC running srsUE, together, form a Software defined radio. The USRP B200mini from Ettus Research acts as the front-end. It upconverts baseband I/Q samples provided by the PC to RF frequency and then transmits them. It also, downconverts downlink RF signal to baseband I/Q samples and provides them to the PC for srsUE to process. The B200mini[8] block diagram is shown in Figure 4.3. The rest/majority of the processes are handled by srsUE on the PC; i.e., synchronisation, decoding data, OFDM FFT/IFFT, and all higher level process such as IP, etc.

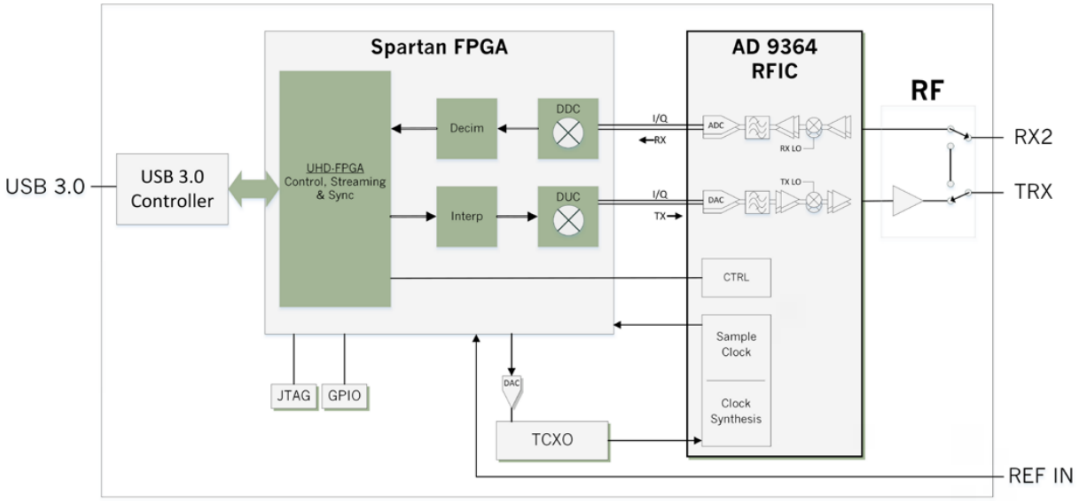


Figure 4.3 Block diagram of the USRP B200mini. It is used as the radio front-end for the software defined LTE UE.

4.4 TEST EQUIPMENT

Figure 4.4 shows the equipment setup used to capture downlink LTE data.

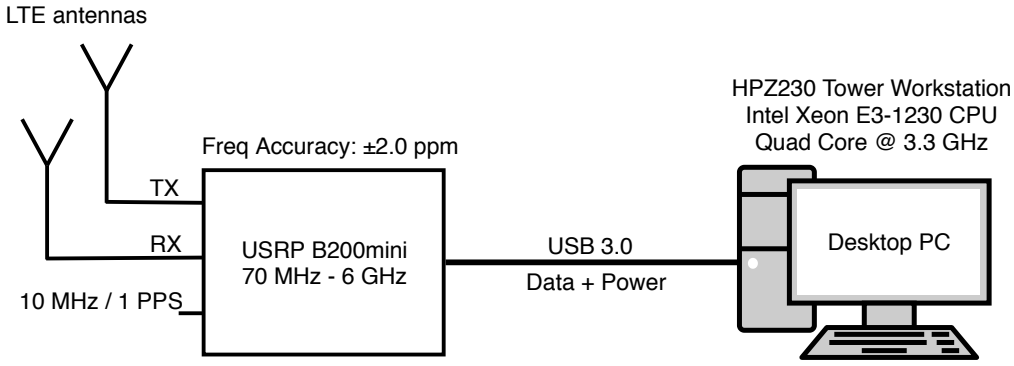


Figure 4.4 Test equipment consisting of two LTE antennas, one USRP B200mini SDR to act as the front end, a USB 3.0 cable for data transfer, and a desktop PC running srsUE — an LTE UE from the srsLTE software suite.

[8]More information on the B200mini is available at: `https://www.ettus.com/product/details/USRP-B200mini`

The minimum hardware requirements of a front-end for srsUE is the following:

- Two antenna ports, one for transmit (TX) and one for receive (RX) is required in order to run srsUE without any modifications. Since this method only relies on downlink data, TX is not necessary for this method. Hence, for a more lightweight program, all srsUE's TX capabilities can be removed in the future and instead an SDR with two RX antennas in diversity mode can be used instead. The B200mini has one TX/RX port and one RX only port and can satisfy this requirement.
- Minimum 30.72 MHz bandwidth. The B200mini has up to 56 MHz bandwidth.
- Gigabit Ethernet or USB 3.0 in order to handle LTE data rates.
- RF frequency covering all LTE bands in the country of interest. In New Zealand band 28 (700 MHz), 3 (1800 MHz), and 7 (2600 MHz) are used. The B200mini has a frequency range of 70 MHz–6 GHz.

4.5 LTE AND ITS PILOT SEQUENCES

This project tests the feasibility of LTE for positioning by analysing the TOA of the Primary Synchronisation Sequences (PSS) and the Secondary Synchronisation Sequences (SSS). Hence, an understanding of these sequences and some knowledge about LTE is important and will be provided in this section.

4.5.1 LTE Frame Structure

The LTE downlink uses the Orthogonal Frequency Division Multiplexing (OFDM) protocol for data transmission which splits the resources in both time and frequency. The LTE frame is 10 ms long and is made up of 10 subframes (SF). Each SF consists of two slots (each 0.5 ms long). Each slot consists of 7 or 6 OFDM symbols depending on whether the network uses the normal cyclic prefix length (L_{CP}) or extended cyclic prefix length respectively. The LTE frame structure is depicted in Figure 4.5

4.5.2 Primary and Secondary Synchronisation Sequences

In LTE, there are two downlink synchronization sequences, used by the UE to obtain the Physical Cell Identity (PCI) of the cell and obtain downlink frame timing. These are the PSS and SSS. The purpose of using two sequences is to reduce the complexity of the 'Cell Search' process[9] [31].

In Frequency Division Duplex (FDD) which most LTE networks use, the PSS is transmitted within the last symbol of the of the first slot of subframes 0 and 5 [19,

[9]The process where the UE searches for an LTE cell to connect to.

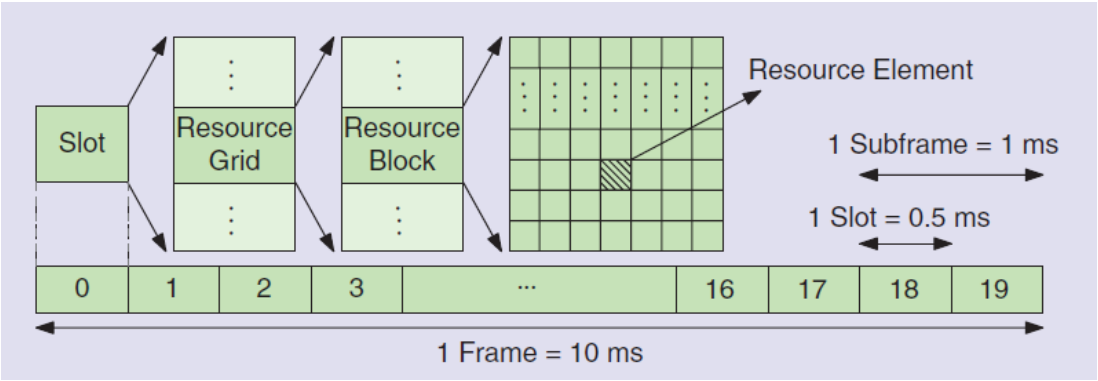


Figure 4.5 The LTE frame is 10 ms long. Each frame is made up of 10 subframes (each 1 ms long). Each subframe is divided into 2 slots (each 0.5 ms long) [25].

pg. 302]. The PSS appears twice in an LTE frame and both are identical. By finding the position of the PSS in a frame, 0.5 ms or half-frame timing can be achieved.

The SSS is transmitted within the second to last symbol of the same slot, i.e., one symbol ahead of the PSS. The two SSS sequences appearing within a frame are different. Hence, 10 ms (i.e., full frame timing) can be obtained by decoding the SSS.

4.5.2.1 PSS Structure

The PSS are length 62 Zadoff-Chu sequences having the property of having zero autocorrelation at all non-zero lags. When used for synchronisation, the auto-correlation has a peak only when the received sequence and the locally generated sequence have zero lag. If there is any lag between the two sequences the correlation is zero [31]. There are 3 different PSS sequences denoted by integers 0 to 2.

4.5.2.2 SSS Structure

The SSS are length 62 orthogonal sequences obtained by concatenating two maximum length sequences scrambled by a third sequence which is generated based on the PSS [25]. There are 168 different sequences denoted by integers 0 to 167.

4.5.3 Physical Cell Identity Extraction

The Physical cell identity (PCI) is defined as

$$N_{\text{id}}^{\text{cell}} = 3N_{\text{id}}^{1} + N_{\text{id}}^{2}\,, \tag{4.17}$$

where N_{id}^{1} is the physical layer cell identity group. Its value is the SSS sequence number (0 to 167) obtained by decoding the SSS. N_{id}^{2} is the identity within the group; obtained by decoding the PSS. Its value is the PSS sequence number (0 to 2). This creates 504 unique PCIs [31].

4.6 OBTAINING LTE TIME OF ARRIVALS WITH SRSUE

In order to obtain the TOA of the SSS, additional lines of code were added to various source files in the srsLTE[10] code base in order to obtain various data required for obtaining SSS TOAs. This data was then written to a file and analysed in post process to determine the suitability of srsUE for positioning.

In order to get timestamps that are reliable, the timestamps must be obtained from the SDR front-end, i.e., the USRP B200mini. The B200mini provides data to PC (i.e., srsUE) one LTE subframe at a time (as requested by srsUE). The LTE subframe is 1 ms long. At 23.04 MHz sampling rate this equates to 23,040 samples per data block. Each block of data sent from front-end includes a header that contains various metadata. The USRP data structure is depicted in Figure 4.6. The header includes the following metadata [35] among others:

- error_code: enum (integer) indicating the error code.
- fragment_offset: positive integer indicating the fragmentation offset. The fragment offset is the sample number at the start of the receive buffer. For non-fragmented receives, the fragment offset should always be zero.
- has_time_spec: bool indicating whether or not a timestamp will be included.
- more_fragments: (bool) fragmentation flag; true when the input buffer has insufficient size to fit an entire received packet. more_fragments will be false for the last fragment.
- time_spec: the timestamp pointing to the first sample in the buffer.

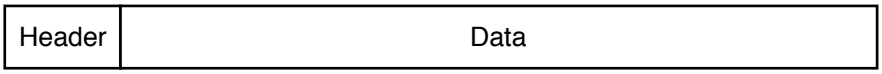


Figure 4.6 USRP SDR data structure. The header contains various metadata including a timestamp pointing to the first sample of the data block.

The following parameters, which were also written to file, were used to determine the TOA of SSS sequences or do other checks:

- sss_idx: integer pointing to the first sample of the SSS sequence within a subframe; i.e., the beginning of symbol 6 after the CP, in subframes 0 and 5. It is an offset, in number of samples, from the beginning of the data block; as depicted in Figure 4.7.
- sf_len: integer indicating the subframe length in number of samples. This depends on the sampling rate. It is 23,040 at 23.04 MHz.

[10]It reads 'srsLTE' and not 'srsUE' because most of the source files modified are also common to srsENB and srsEPC which are also part of the srsLTE software suite.

- db_ts: timestamp pointing to the first sample of the data block provided by the front-end. One timestamp is provided for each data block.
- sf_idx: subframe index; i.e., the number of the current subframe. Each frame contains 10 subframes, hence, this value cyclically repeats from 0 to 9. It is used to check for subframes 0 and 5 (where the SSS appears).
- nsamples: integer indicating the number of samples, requested by the PC, per data block.
- rxd_nof_samples: integer indicating the number of samples received by the PC. This is required to ensure that the SDR provides the exact number of samples requested in nsamples.

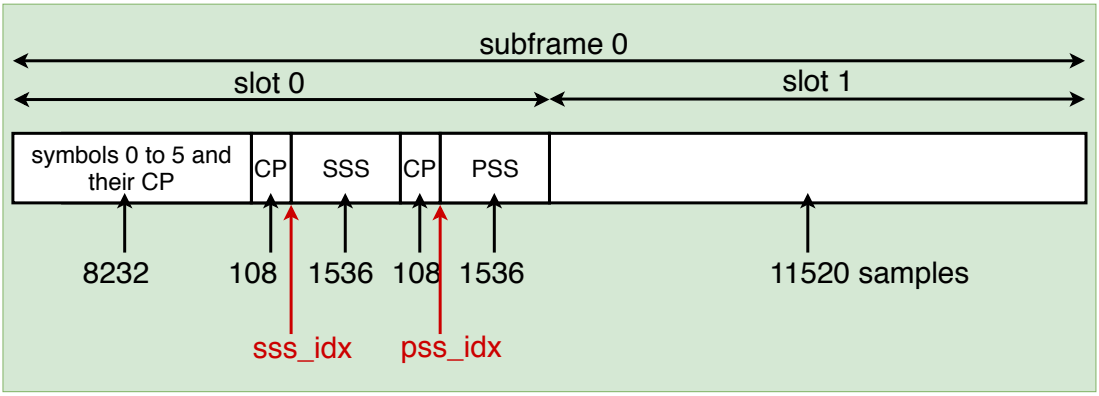


Figure 4.7 The SSS and PSS index (location) within subframe 0; they appear in the same locations in subframe 5. The SSS index points to the beginning of symbol 6 (after the CP) where the SSS appears. The PSS appears in the following symbol and, hence, the PSS index points to the beginning of the next symbol (after the CP). It also shows the number of samples each sequence is made of; i.e., 1536 samples. NOTE: The sss_idx is the location of the peak of the autocorrelation of the SSS sequence within the data block. That is, it is an offset from the beginning of the data block obtained from the B200mini. Although the data block is generally 23,040 samples (1 subframe), the beginning of the data block is generally not the beginning of the subframe. Hence, the sss_idx is not a constant.

The TOA of the SSS sequence, represented by a timestamp pointing to the first sample of the sequence, sss_ts, is calculated using the equation

$$\text{sss\_ts} = \text{db\_ts} + \text{sss\_idx} \times T_s \,, \tag{4.18}$$

where, T_s is the sampling period, equal to $1/23.04 \times 10^6 6$ at 23.04 MHz sampling frequency.

4.7 THE EXPERIMENT

For the LTE pilot sequences to be useful for positioning they must be periodic with a strict period, which in the case of LTE, is specified as 5 ms. The first check in this

project is to confirm that this is the case. This can be done by analysing the period of the SSS TOAs when the UE is stationary. If this is the case, each sss_ts (calculated from Equation 4.18) should arrive exactly 5 ms apart.

This experiment was carried out in an office, with both LTE antennas placed near a window and sufficiently far apart from one another. The SSS TOAs were obtained using the method described in Section 4.6. The difference between consecutive sss_ts were computed and stored an array. A histogram of the array is plotted in Figure 4.8, showing the average time difference between SSS TOAs.

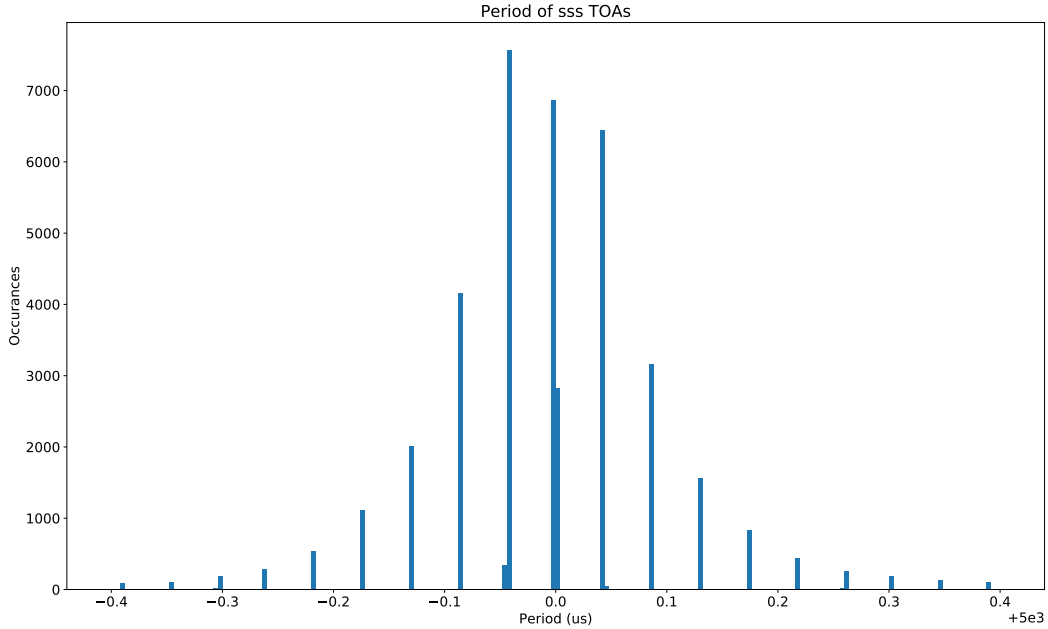


Figure 4.8 A histogram of the period of SSS TOAs (aka sss_ts). The period is shorter than 5 ms, typically by 6 ns, depending on the trial.

As shown in Figure 4.8, on average each SSS sequence appears slightly less than 5 ms after one another. This is indicated by the mean and peak of the histogram. The mean is at 4999.9945 μs instead of at 5000 μs; i.e., 5.5 ns less. The largest peak appears one T_s (43.4 ns) before 5000 μs instead of being at exactly 5000 μs. The standard deviation (1σ) of the TOAs from the mean is 127 ns.

4.7.1 Multipath Effects

The peaks around the central peak in Figure 4.8 show the imprecise detection of the TOA of SSS sequences. The fact that there is not a single peak shows that srsUE is not able to precisely detect the TOA every time. The standard deviation (1σ) of 127 ns equates to a distance error of 38.1 m; or 76 m (2σ).

The data plotted in Figure 4.8 was captured from a UE situated inside a building made of many metal structures especially near the window where the LTE antennas

were situated. There are also some large trees near the window. Hence, the cause of such large deviations in the detection of SSS TOAs is likely due to multipath, which is very likely in an environment with many obstructions. This environment is shown in Figure 4.9.

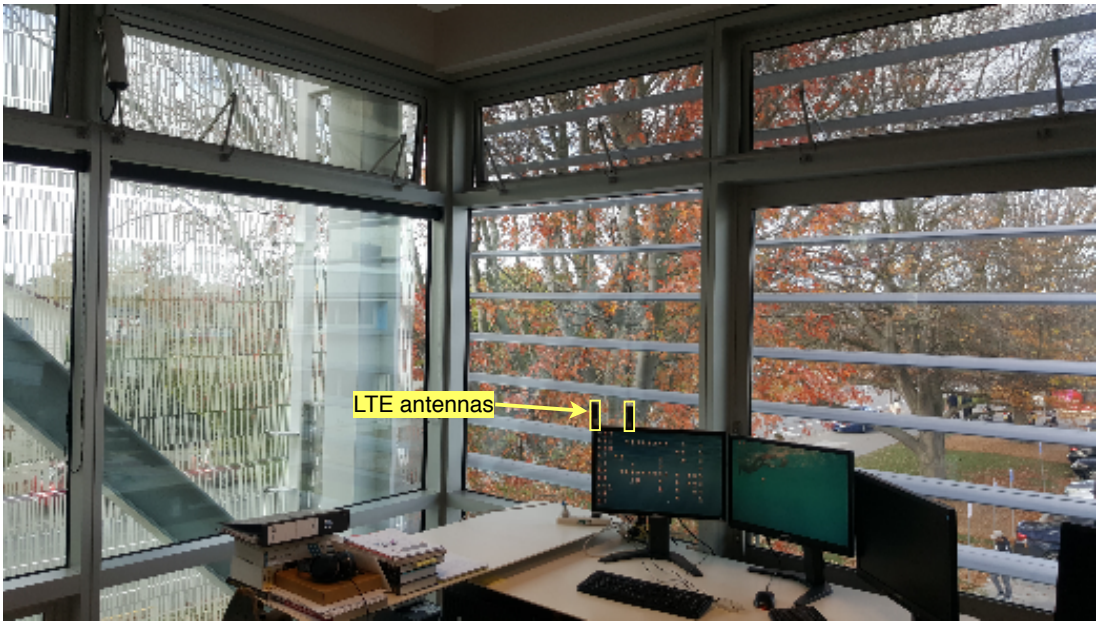


Figure 4.9 UE antennas situated near a window inside a building made of lots of metal structures, and a few large trees outside, causing signal degradation and multipath.

When the LTE antennas were attached to the windscreen of a car moving towards an eNB, where the multipath was much less, the errors were noticeably smaller and typically resulted in standard deviations of ∼65 ns. This equates to a distance error of 19.5 m (1σ) or 39 m (2σ)[11]. In this environment (see Figure 4.10), although there was less multipath, some multipath was still present since the road was narrow and surrounded by trees and houses. Nevertheless, a standard deviation of 39 m (2σ) is satisfactory. Placing the UE on a UAV should result in even less multipath, and provide even better results.

[11]The histograms of these trials are not shown as they looked nearly identical to the histogram in Figure 4.8, hence, providing little information to the reader even though the standard deviations were much smaller.

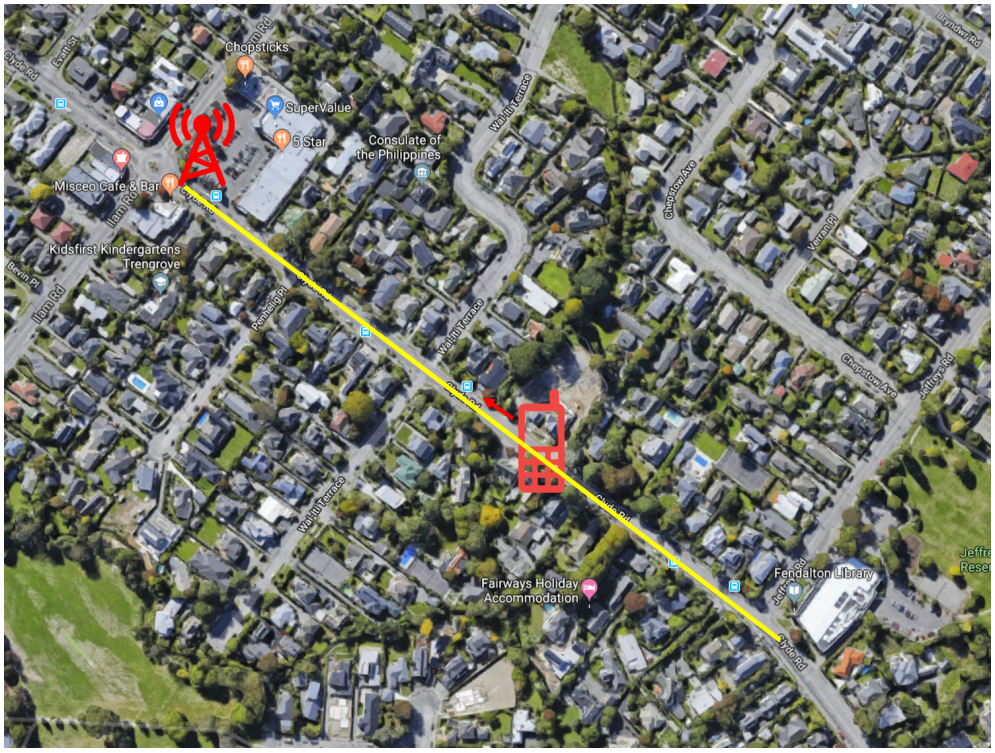


Figure 4.10 A birds eye view of the environment of the UE as it was moving towards the eNB. The road was surrounded by many houses and trees; although these are low lying, they still cause some multipath, but much less than when the UE is situated inside a building. The yellow line marks the path of the vehicle and the red arrow the direction of travel (i.e., towards the eNB).

4.7.2 Time Drift of UE and eNB Clocks

Figure 4.8 showed a mean SSS TOA period of 4999.9945μs (5.5 ns less than 5 ms). For the SSS period to be exactly 5 ms, the eNB clock must be perfectly accurate, i.e., perfect precision and no time drift. In reality the eNB clocks will not be perfect, hence, the actual period of transmission of SSS sequences will depend on the accuracy of the eNB clocks used. All eNBs owned by the Spark network (a New Zealand based mobile service provider) have high precision Oven Controlled Xtal[12] Oscillators (OCXO) which are disciplined by GPS [42]. Hence, while the eNB is locked to GNSS, the SSS period will be, more or less, exactly 5 ms. It is reasonable to assume that this is the case since GPS availability in first world countries is typically near 100 %.. Hence each SSS should be transmitted, on average, exactly 5 ms after one another. But, this is not reflected in Figure 4.8.

The reason for this is likely because the UE clock is slower[13] . If this is the case, even if the sequences are transmitted every 5 ms exactly, it will not appear that way at the UE; which timestamps the arrival of the sequences based on its own clock's timing.

[12]Xtal is an informal abbreviation for crystal.
[13]That is, it oscillates at a slower rate than the rate specified.

The UE clock is a low quality 40 MHz temperature compensated crystal oscillator (TCXO). Hence, to the UE, 40 million ticks is one second. If the actual clock-rate (frequency) is lower, each tick will be longer, such that slightly less than 40 million ticks will make up one second. But the UE does not know this, and hence, counts 40 million ticks to get one second.

According to Figure 4.8, the UE clock falls behind the eNB clock by 5.5 ns every 5 ms; which equates to a time-drift[14] rate of -1.1 μs/second (μs/s).

Figure 4.11 shows the time drift of the UE clock from the eNB clock. Considering that the eNB's OCXO is significantly more accurate than the UE's TCXO and also disciplined by GPS, it should have zero long term[15] drift from actual time; i.e., GPS time or UTC. Hence, the majority of the time drift shown in Figure 4.11 is likely to be from the UE clock. The gradient (i.e., time drift rate) of the graph is -1.1 μs/s; which is consistent with the results obtained from Figure 4.8. The negative gradient indicates that the UE clock is slower than the eNB clock and will fall behind over time.

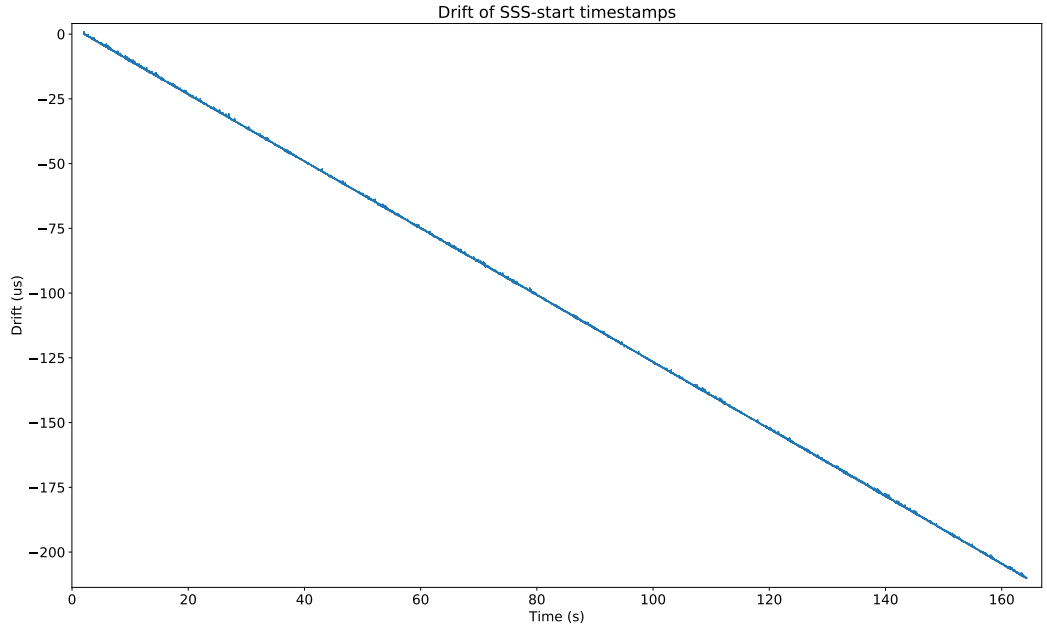


Figure 4.11 The UE clock's time drift with respect to a commercial LTE eNB clock (when the UE is stationary). The negative gradient of the graph indicates that the UE clock is slower than the eNB clock, hence its time will lag behind the eNB clock's time. A curve showing no drift would always have a value of 0 (i.e., 0 drift) — although slight fluctuation (i.e., noise) due to the imprecise detection of SSS TOAs would still be present. This noise is better shown in Figures 4.12 and 4.13 which are closeups of this graph.

[14] "Time drift" is the amount of time a clock's value has deviated (i.e., drifted) away from another clock or from actual time.

[15] I.e, more than a few seconds. A clock which is disciplined by GPS typically has its time corrected every second by the pulse-per-seconds (PPS) signal from the GPS receiver.

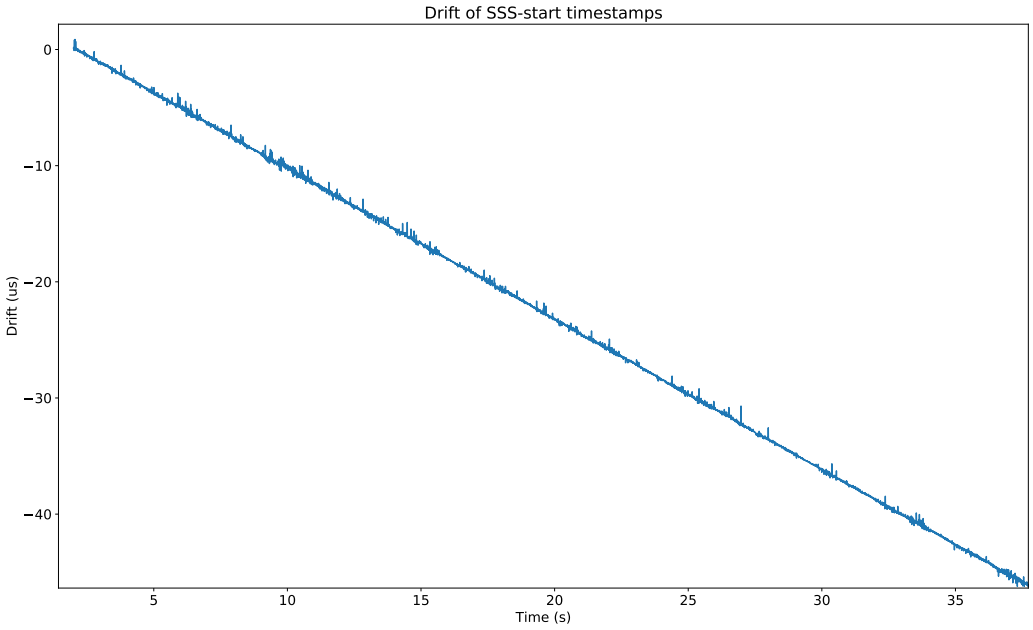


Figure 4.12 Closeup of Figure 4.11 showing the noise of the drift graph caused by the imprecise detection of SSS TOAs.

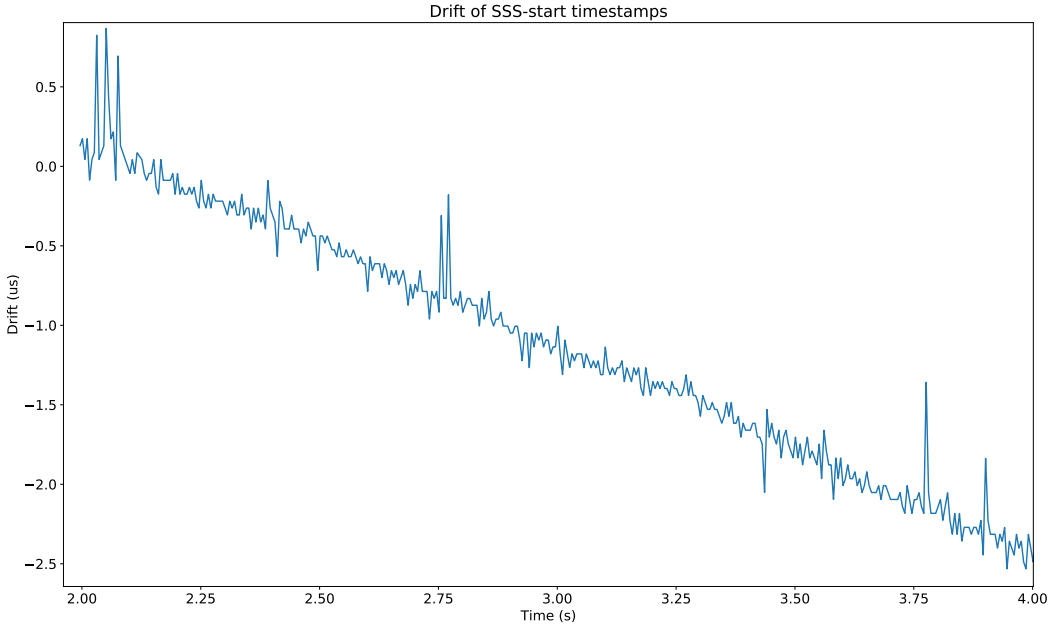


Figure 4.13 A close-up of Figure 4.13, showing the noise of SSS TOAs due to multipath. Multipath is caused by obstructions (metals structure, trees, etc.) present around the UE. The large noise spikes can be removed with filtering.

The drift (i.e., time drift[16]) data plotted in Figures 4.11–4.13 were obtained in the following way: An array, A, consisting of SSS TOAs (i.e., sss_ts) were obtained

[16]Since this thesis only mentions drift with respect to time, the term drift will always refer to time drift. Hence, both terms will be used interchangeably throughout this thesis.

from srsUE. The array takes the form $A = \{t_0, t_1, t_2, ..., t_n\}$, where $t_0, t_1, t_2, ..., t_n$ are consecutive SSS TOAs. The following operations were done in Python on array A to obtain array B which contains the time drift data plotted in Figures 4.11–4.13:

```
B = (A[0:] - A[0]) % 5e-3
B = B * (1e6) # Convert unit from seconds to microseconds.

# Get drift
for i in range(len(B)):
    B[i] -= 5000
```

4.7.3 Drift Compensation

A drift rate of $-1.1\,\mu$s/s (determined from Figure 4.11), indicates that in n seconds, the UE clock's time will have drifted from the eNB clock's time by $-1.1 \times n$ microseconds. Considering that each microsecond causes a distance error of 300 m[†], this can be detrimental to positioning, and hence, must be estimated and removed. A linear drift rate such at the one shown in Figure 4.11 can be approximated by an equation of the form

$$y = mt + c\,, \tag{4.19}$$

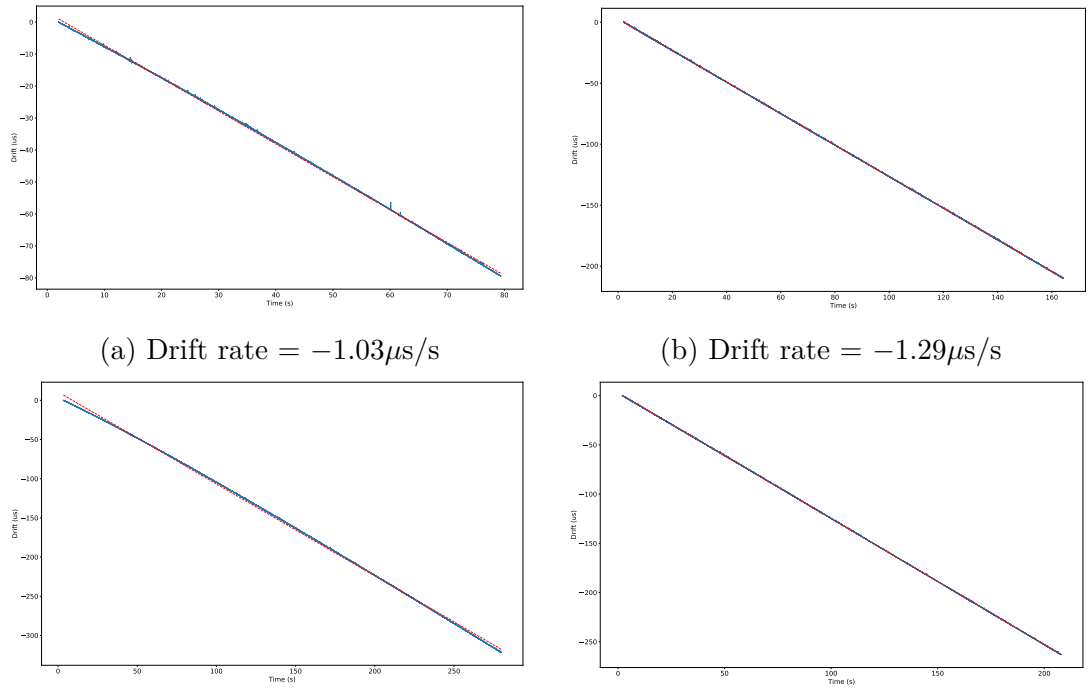
where,

- t is the amount of time that has elapsed since t_0 (the initial TOA),
- m is the gradient or rate of time drift,
- y is the total time drift t seconds after the initial TOA, and
- c is a fixed offset, representing the initial time bias (at t_0) between the eNB and UE clock. This can be assumed to be 0.

Although Figure 4.11 shows a linear drift rate, TCXOs are not very stable and generally have a non linear (usually parabolic) time drift. A trial time of ∼160 s (see Figure 4.11) is also rather short. Over the period of tens of minutes or an hour the non-linearity of low quality clocks become clearly visible. This non-linearity is evident from Figure 4.14 (a) and (c) where after trails of 80 seconds and 250 seconds respectively the non-linear time drift of the UE clock (blue line) is clearly visible; note the deviation time drift from the red-dashed linear trend line. TCXOs are also highly temperature dependant. Although, the name 'TCXO' implies that temperature effects are compensated, without ovenising the crystal, precise temperature compensation cannot be achieved.

[†] $(1 \times 10^{-6})(3 \times 10^{8}) = 300$ m.

The trials of Figures 4.14 (a)–(d) were taken within a span of ∼20 minutes, and each show significantly[17] different drift rates. These large volatilities in drift rates and non-linearities will make drift compensation difficult and likely impossible.



(a) Drift rate = -1.03μs/s

(b) Drift rate = -1.29μs/s

(c) Drift rate = -1.17μs/s

(d) Drift rate = -1.28μs/s

Figure 4.14 The time drift rates of the B200mini TCXO over a period of ∼20 minutes. (a) Drift rate of -1.03μs/s immediately after device (i.e., B200mini) start-up when the device was at ambient temperature. (b) Drift rate of -1.29μs/s 3 minutes after device start-up. The device was completely warmed up at this stage and the temperature difference between trials b to d were unnoticeable to the touch. (c) Drift rate of -1.17μs/s 7 minutes after device start-up. (d) Drift rate of -1.28μs/s 13 minutes after device start-up. The graphs shows that the drift rate of the b200min TCXO can change significantly over a short span of time.

4.7.4 Practical Accuracy

Based on the results obtained so far, in a low multipath environment e.g., when the UE is situated on a UAV, the UE should be able to localise itself with an accuracy of better than 39 m (2σ). In regions with severe multipath, such as inside buildings or in urban canyons the accuracy will be worse. The amount of accuracy degradation will depend on the level of multipath.

The accuracies stated above, will only be possible if the UE and eNB clock's time drift is compensated. When using low quality clocks, e.g., a TCXO, the time drift rate will be on the order of microseconds. Hence, the errors of the system will be dominated by time drift errors; since a drift rate of 1 μs/s causes a distance error of 300 m/s. Without compensation, the system will quickly fail.

[17] That is, significant for positioning.

By removing the effects of multipath, the SSS TOAs can be detected with higher precision thus improving the accuracy of the system. A possible solution for removing multipath effects is provided in [24] which operates on the TOA of the Cell-specific Reference Signals (CRS) instead of the TOA of SSS — which should enable T_s (13 m) level accuracy.

Additionally, by using the Francois Blais and Marc Rioux peak detector algorithm [15], or by over-sampling, the TOA of pilot sequences can be detected with sub T_s resolution. With multipath effects removed, this may enable the system to achieve an accuracy of better than 13 m.

4.8 THE NEED FOR HIGH QUALITY CLOCKS

It is evident from Figure 4.14 (a)–(d) that low quality clocks are unstable, and hence, inaccurate. Their time drift is non-linear, temperature dependent, and have a large rate of change.

In order to compensate for the time drift of a clock, the time of the clock must be monitored against a superior clock such as a Rubidium-Standard or a GPS-Disciplined Oscillator (GPSDO) for an extended period of time (e.g., 12+ hours) and over several trials to ensure that the model obtained from each trial is consistent with one another. If a different model is obtained with each trial, that model is unlikely to be useful. Based on the model, the clock's time drift can be compensated by making small adjustments to the operating frequency of the clock or periodically adding a correction value so that it shows the right time.

Considering the non-linearity and volatility of the time drift of low quality clocks, obtaining an accurate model of its time-drift is likely not possible. Hence, a higher quality clock such an GPS-Disciplined (GPSD) OCXO will likely be a necessity for a practical system. A GPSD-OCXO's time does not drift while locked to GPS. When GPS lock is lost, its accuracy will depend on the accuracy of its OCXO, which has a much higher accuracy than, for example, a TCXO. An OCXO's time drift is also linear over a longer time compared to the time drift of a low quality clock (i.e., for several hours depending on the quality of the OCXO). Because of its higher frequency stability, the rate of its time drift is also smaller. Hence, its time drift would be easier to model and compensate.

It is obvious at this stage in the report that having accurate timing is crucial to positioning and that a high quality clock is likely a necessity, both for the eNBs and UE, in order to realise a practical positioning system. The following sections will mostly be about clocks and timing to emphasise the importance of accurate timing in positioning and determine the level of quality required in a clock.

Section 4.8.1 will discuss clock stability and time drift, and the factors that affect

them. Section 4.8.3 will discuss the reliability time of a positioning system in the absence of GNSS and with no drift compensation when the UE is equipped with a relatively high quality OCXO. Sections 4.8.4 and 4.8.5 provide examples of clocks, both for the UE and eNB, so that for the entire duration of the UAVs flight (∼1 hour), time drift can be completely ignored; which may be critical for scenarios where drift compensation is either not possible or cannot be relied on. Conclusions are provided in section 4.8.6.

4.8.1 Clock Stability and Time Drift

The aim of this section is to explain the concepts of clock stability and time drift, and how they can be determined from the specifications of a clock.

The frequency accuracy/stability[18] of an oscillator (i.e., clock) is generally given in parts per million (ppm) or parts per billion (ppb). The frequency stability of a clock depends on various factors [27]; namely the following:

- **Initial offset or frequency tolerance:** The initial offset depends on the quality of the crystal's cut, impurities in the crystal's growth, and uneven thickness of the processed crystal, leading to slight differences in the nominal frequencies of a batch of crystals. This is usually specified at 25 °C.
- **Frequency over temperature:** As the temperature of the crystal varies, the frequency of the oscillator will also vary.
- **Supply voltage:** Fluctuations in the operating voltage of the crystal can change the frequency of its oscillations.
- **Aging:** Crystals are electromechanical devices, and hence, subject to many internal and external environmental factors.
- C_L **mismatch:** The oscillation frequency of a crystal depends on its load capacitance and will be affected by the tolerance of the loading capacitors over the temperature range. It is usually expressed in ppm/pF of capacitance variation.

Overall frequency stability, $F_{\text{stability}}$, is a cumulative value [27], i.e.,

$$F_{\text{stability}} = F_{\text{tolerance}} + F_{\text{temp}} + F_{\text{voltage}} + F_{\text{aging}} + F_{\text{load}}\,. \tag{4.20}$$

The error of an oscillator from its nominal frequency, in ppm or ppb, are given by the following equations [27]:

$$\text{ppm error} = \frac{F_{\text{actual}} - F_{\text{nominal}}}{F_{\text{nominal}}} \times 10^6 \tag{4.21}$$

[18]The terms frequency accuracy and frequency stability are often used interchangeably, since a high accuracy clock must have high stability, and vice versa.

$$\text{ppb error} = \frac{F_{\text{actual}} - F_{\text{nominal}}}{F_{\text{nominal}}} \times 10^9 \tag{4.22}$$

From the ppm or ppb error, an oscillator's output frequency variation (in Hz) from its nominal frequency can be calculated using the equation,

$$\text{variation in Hz} = \frac{F_{\text{nominal}} \times \text{ppm error}}{10^6}\,. \tag{4.23}$$

For example, if an oscillator specifies a nominal frequency of 10 MHz and a frequency stability of ±5 ppm, its actual frequency may deviate from 10 MHz by a maximum of ±50 Hz.[19]

Since an oscillator determines time by counting its oscillations, if the oscillator's actual frequency is not equal to its specified nominal frequency, the resulting time will have an error added to it that is proportional to the offset between the actual and nominal frequency of the oscillator. This offset, will cause the oscillator's time to drift away from actual time. The total drift[20] can be calculated using the equation

$$\text{drift}(T) = \sum_{t=0}^{T} \frac{\text{variation\_in\_Hz}}{F_{\text{nominal}}} \times t\,, \tag{4.24}$$

$$= \sum_{t=0}^{T} \frac{F_{\text{actual}} - F_{\text{nominal}}}{F_{\text{nominal}}} \times t\,, \tag{4.25}$$

where, drift(T) is the total time drift accumulated over a period of T seconds.

NOTE: The frequency error (e.g., in ppm) on a datasheet specifies the maximum error of the oscillator from its nominal frequency. Hence, calculating drift from the ppm error will give the maximum drift. In practice, a oscillator's actual time drift is found by comparing its time with a more accurate clock, e.g., a Rubidium Standard or a high precision GPSDO.

4.8.2 The Oven Controlled Crystal Oscillator

The OCXO is an example of a high quality clock which minimises many of the factors that increase the instability of an oscillator. They come in a wide range of accuracies but the highest quality typically use a Stress Compensated (SC) cut crystal. SC cut crystals are high precision cut quartz crystals, cut in a certain way to reduce or eliminate stress induced frequency shift. As a result, SC cut crystals are less sensitive to mechanical and vibrational stresses, have better aging (<2 ppb/day), and faster warmup time compared

[19] $(10 \times 10^6) \times 5/10^6 = 50$

[20] From this point onwards the term 'drift' will always be used to refer to time drift.

to AT cut crystals. SC cut crystals also have higher Q, resulting in lower phase noise [17].

Lower quality oscillators typically use AT cut crystals since they are cheaper and easier to manufacture. AT and SC cut crystals have different stability curves. While both have a third-order frequency dependency (see Figure 4.15) with temperature, the inflection temperature of SC cut crystals is higher at around 92 °C compared to the 25 °C inflection temperature of AT cut crystals.

Around their inflection temperature, i.e., near the hot end, SC cut crystals have much better frequency stability over a wide temperature range, but tail off quickly on the cold end. Hence, they are more suitable for OCXOs where the crystal is placed inside an oven and its temperature is regulated between 80–100 °C. Around this region, temperature variations in the oven cause less frequency change compared to AT, and most other, crystal cuts [17].

Due to their lower sensitivity to mechanical and vibrational stresses, SC cut crystals are also more suitable for use on aircraft [17].

The disadvantage of SC cut crystals is that they are much more expensive since the manufacturing costs are higher due to more labour and poorer yields over AT[21] cut crystals [17].

[21] Most common crystals are AT cut. These are much cheaper as the cut requires less precision. They also have good performance over a wide temperature range (−55 °C to 125 °C).

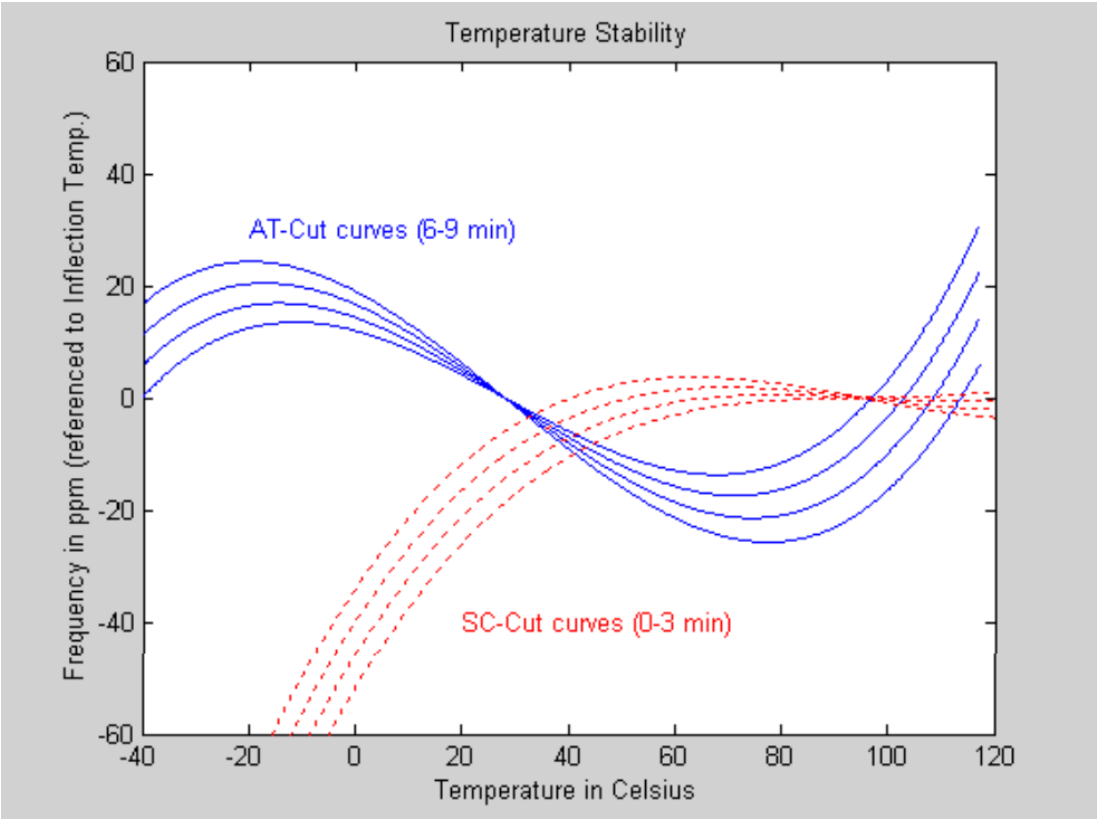


Figure 4.15 Frequency stability over temperature of AT and SC cut crystals. The SC-cut crystal has better frequency stability around its inflection temperature of 92 °C; the temperature at which it is ovenised. Around this point the stability curve is flatter, and hence, the frequency varies little with temperature changes resulting in superior frequency stability. The AT cut crystal is ovenised near its local minimum, but the frequency stability vs temperature curve is not as flat around this point. Hence, it is less stable over temperature. Thus, the SC cut provides better short term stability, as a result of temperature transients within the oven, compared to the AT cut [17].

4.8.3 System Reliability in a GNSS Denied Scenario with no Drift Compensation

A useful thing to know is how long it will take an LTE SDR localisation system's clock drift to reach an error of 100 m, in the absence of GNSS and without drift compensation using a high quality COTS[22] OCXO.

Since the UAV will mostly use GNSS for localisation it will have a GNSS receiver. If both a GNSS receiver and OCXO are required, the best option is to simply to use a GPS disciplined OCXO. Hence, when GNSS is available the OCXO will not drift. The specifications of a typical GPSDO such as the USRP N210 GPSDO[23] will be used for this analysis.

[22] COTS: Commercially available Off The Shelf.

[23] The N210 GPSDO is used for this example as it was the only GPSDO available at the office, but, it was not used in the project due to its incompatibility with the B200mini front-end. The GPSDO's datasheet is available at: `https://www.ettus.com/all-products/gpsdo-kit/`

The parameter of interest here is the N210 GPSDO's 'holdover' time, which is specified as $<\pm 11\,\mu$s over 3 hours at 25°C. This specifies that if GNSS become unavailable at t=0, 3 hours later at t=3 hours, the time of the OCXO will have drifted by less than 11 μs.

11 μs over 3 hours indicates a drift rate of 1.0185 ns/s, assuming linear drift. When the total drift reaches 333 ns, a distance error of 100 m[‡] will be reached (the maximum allowable error). At a rate of 1.0185 ns/s it would take 327.13 s (5.5 minutes), without drift compensation, for the errors to reach 100 m. This is under the assumption that the eNB clock has no drift, i.e., all drift comes from the UE clock (as depicted in Figure 4.16).

In reality this will not be the case. Both the UE and eNB clocks will have some drift in the absence of GNSS. The worst case scenario will be when one clock is slow (relative to actual time) and the other is faster; as depicted in Figure 4.17. In such a scenario the errors will grow faster compared to the scenario depicted depicted in Figure 4.16.

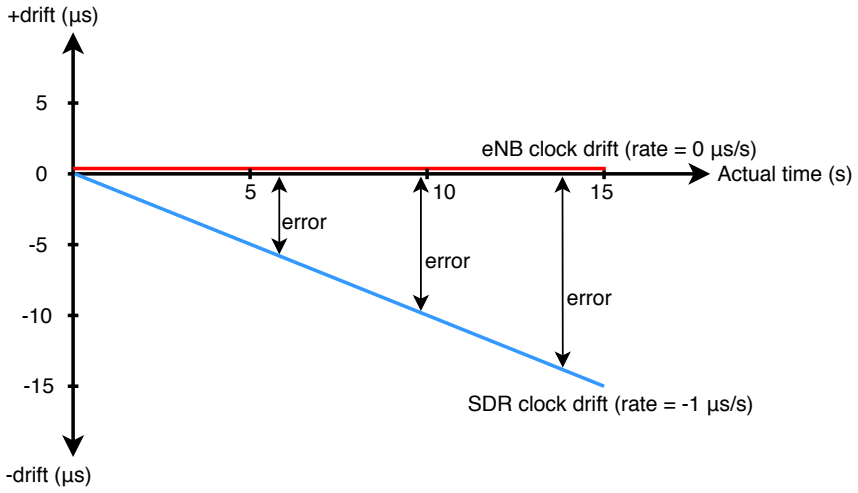


Figure 4.16 A scenario where the eNB clock does not drift; i.e., all the drift comes from the UE clock. Assuming the UE is equipped with the N210 GPSDO, and has a linear drift rate of 1.0185 ns/s, it would take 5.5 minutes for the positioning errors to reach 100 m.

Assuming both the UE and eNB are equipped with the N210 GPSDO, and one has a drift rate of 1.0185 ns/s and the other has a drift rate of -1.0185 ns/s, the positioning errors of the UE will reach a 100 m in half the time (2.75 minutes instead of 5.5 minutes) compared to the scenario depicted in Figure 4.16.

Is it clear from these results that a typical GPSDO such the USRP N210 GPSDO, although high quality and rather expensive ($908.37 USD [6]), is not suitable for a full flight without GNSS and compensation.

Although, 2.75 minutes might be enough time for an emergency landing, higher

[‡] $(333 \times 10^{-9})(3 \times 10^{8}) \approx 100\,m$.

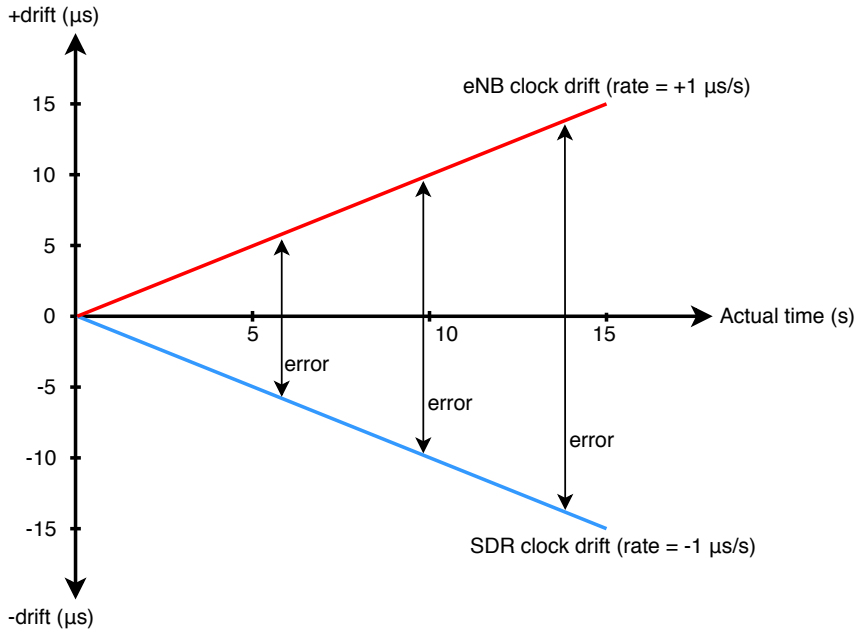


Figure 4.17 A scenario where the UE and eNB clocks drift rates are equal and opposite (in sign); e.g., one drifts at 1.0185 ns/s and the other at -1.0185 ns/s. The overall time drift of the system, from actual time, will be twice as much as the scenarios depicted by Figure 4.16.

quality clocks than even the N210 GPSDO will required in order to ensure that the positioning errors of the UAV will be less than 100 m over its entire flight time. Otherwise the system must have a robust drift compensation algorithm that is capable of estimating and compensating both the UE and eNB's clock drifts.

4.8.4 OCXO with holdover of 1.5μs over 24 hours

A much higher quality clock, compared to the N210 GPSDO is the IQCM-100[§] GPS disciplined OCXO from IQD [34]. Although more expensive (~$1,500 USD), under the right conditions it can provide a holdover of 1.5μs over 24 hours. It is able to achieve this level of accuracy by using "an algorithm [that] enables adaptive modelling of the frequency stability of the OCXO with reference to the GPS timing signal". But it is only able to do this if the device has been on for seven day with two days of good GPS signal [34].

A 1.5μs drift over a 24 hour period is equivalent to a drift rate of 0.017361 ns/s. At this rate, it would take the clock 5.33 hours to accumulate a timing error equivalent to a distance error of 100 m.

Although a UE situated on a UAV is unlikely to achieve seven days of on time with two days of good GPS signal, in order to achieve the specified holdover, it should be easy for a base station which is always stationary and located at high altitudes with

[§]IQCM-100 datasheet: `https://www.iqdfrequencyproducts.com/products/details/iqcm-100-2-34.pdf`

good LOS access to GPS signals. It is unknown at this stage (and unlikely) that LTE eNBs use such high quality clocks. It is likely too expensive and also unnecessary (for communications). Nevertheless, if it were to use it, timing errors resulting from the eNB clock could be virtually ignored for the entirety of a UAVs flight, especially since the flight time of fully electric VTOL UAVs is likely to be no more than ∼60 minutes.

4.8.5 Chip Scale Atomic Clock GPSDO

Although the GPS disciplined OCXO mentioned in the previous section (4.8.4) is a very high quality clock, it is unlikely to be suitable for a UAV. Due to the constant movement of the UAV from place to place, it is unlikely to meet the required holdover conditions; i.e., seven days of on time with two days of good GPS signal.

A technically feasible option for the UE is a Chip Scale Atomic Clock (CSAC) GPSDO, e.g., the Jackson Labs CSAC GPSDO[24] which has a small form factor ($2.5 \times 3.0 \times 0.7$ inches) and consumes <1.4 W of power. It has a holdover stability (after 96 hours of warmup) of $<\pm 2\,\mu$s over a 24 hour period at 25°C after 20 minutes of GPS lock [7]. The main advantage of this is that it only requires 20 minutes of GPS lock to achieve its specified holdover. Assuming a linear drift rate, $2\,\mu$s over 24 hours equates to a drift rate of 0.023 ns/s. At this rate, it would take the clock 4 hours to accumulate a timing error equivalent to a distance error of 100 m.

The cost of the Jackson Labs CSAC GPSDO is $4,285.00 USD.

4.8.6 Constituents of a Reliable System with no Drift Compensation

By equipping all eNBs with clocks of quality similar to the IQCM-100 (see Section 4.8.4) and the UAVs with CSAC GPSDOs (see Section 4.8.5), the resulting positioning system should enable the UAVs to operate, in the worst case scenario as depicted by Figure 4.17, for ∼2.3[¶] hours before the distance errors due to the overall time drift of the system exceeds 100 m.

Considering the short flight time of fully electric VTOL UAVs and that GNSS signal availability in developed parts of the world is near 100 %, there should be few situations requiring the operation of any backup positioning system for more than tens of minutes without GNSS. In the rare case where a UAV is required to operate for the full duration of its flight time without GNSS, 2.3 hours should be enough for the UAV to safely complete its journey. If even a single reliable GNSS fix is obtained during holdover, e.g., when GNSS signals are intermittent, the UAV will be able to reset any positioning errors accumulated from time drift.

[24] SCAC datasheet: `http://www.jackson-labs.com/assets/uploads/main/CSAC_specs1.pdf`

[¶] $(1/5.33 + 1/4)^{-1} \approx 2.3 hours.$

The system described here is likely the only option for a reliable LTE SOP based positioning system without having to implement any complicated algorithms for estimating and removing the time drift of eNB and UE clocks; especially if drift compensation is either not possible or cannot be relied on.

4.9 IMPLEMENTATION FEASIBILITY

It is likely feasible to detect LTE TOAs with high precision (as done by [37] and [20]) and likely possible to remove multipath (solution is provided in [15]). The largest issue will likely arise from time drift. A possible solution to mitigating drift is given in Section 4.8.6 which involves equipping the eNBs with high quality GPS-disciplined OCXOs such as the IQCM-100 and the UAVs with CSAC GPSDOs. This results in a positioning system where the distance errors, resulting from time drift, will be less than 100 m for at least 2.3 hours. Hence, over a flight time of ∼1 hour (typical for a VTOL UAV), the total system errors resulting from all factors (i.e., time drift, multipath, and quantisation errors in the detection of TOAs), is likely to be less than 100 m.

While it may be possible to justify equipping a UAV with a $4,300 USD CSAC GPSDO, equipping all eNBs with expensive ($1,300 USD) IQCM-100s, in case the holdover of the current eNB clocks are inadequate for positioning (which is not known), will be either impossible, or difficult to achieve, and will require collaboration with mobile service providers.

If the cost of a CSAC GPSDO for a UAV is too high to justify, the UAV can be equipped with a GPS-disciplined OCXO instead. High quality OCXOs are very stable. Hence, their time drift should be possible to model and compensate. When the UAV is locked to GNSS, be it in flight or out of flight (i.e., night time, or when not operating), an algorithm similar to the one used by the IQCM-100 can be used by the UAV to continually monitor the drift of its OCXO with respect to GPS time, and dynamically model it. During operation, if GNSS lock is lost, the model can be used to estimate and compensate the UAVs clock drift.

If the current eNBs clocks are regular GPS-disciplined OCXOs with similar specifications to the N210 GPSDO,[25] their time drift will reach an error of 100 m in around 5 minutes without drift compensation (see Section 4.8.3). Modelling an eNB clocks time drift will be difficult. Since the eNB OCXOs are continually disciplined by GPS, their drift cannot be monitored to create a model. Hence, their drift cannot be compensated in the absence of GNSS.

Hence, the feasibility of an LTE SOP based positioning system, will depend, mainly on whether eNB clock drifts can be mitigated or not. Although a system which is

[25] The oscillator of the N210 GPSDO is an OCXO.

reliable for around 5 to 10 minutes should be possible, and can be useful for emergency landings.

4.10 PRACTICAL POSITIONING RESULTS

The time drift of a low quality clock such as the TCXO used by the B200mini, although mostly linear in the tests carried out in this project, resulted in varying drift rates with each trial. The source of such volatility in drift rates (see Figures 4.14 (a)–(d)) is not exactly known, but it likely due to errors from both the temperature changes in the crystal and the inherent instability of the TCXO.

Moving towards or away from an eNB has the effect of increasing and decreasing the drift rate of the UE clock respectively. One way of separating (and removing) the actual drift from the apparent 'drift' caused by the motion of the UE, is to measure the drift of the UE clock when it is stationary and then subtract it from the drift of the UE clock which is moving. With the actual drift removed, the remaining "drift" would be from the motion of the UE; which can be used for getting the distance between the UE and eNB.

While this seems like a simple task, considering the volatility of the UE clock's drift rate from trial to trial, it was not possible in the case of this project. This is likely possible with a higher quality clock such as an OCXO whose drift rate will likely remain constant from one trial to the next. Otherwise it would be difficult to know whether the drift rate observed when the UE is stationary will be equal to the drift rate in a subsequent trial where the UE is moving.

In order to determine a more credible figure for the practical accuracy of the system, than that given in Section 4.7.4, obtaining practical positioning results is a necessity. But this is likely only possible with a higher quality clock.

4.11 PITFALLS

This section discusses some the pitfalls that were encountered during this project. It is provided to the reader so that they may avoid the same issues. They are the following:

1. **Not specifying timestamp decimal places**
   Timestamps in srsUE have two components, i.e., $full\_secs$ and $frac\_secs$. Consider the timestamp 3.1234567891011 seconds. The full seconds part or 3 is stored in $full\_secs$, which is a long integer. The fractional part or 0.1234567891011 is stored in a double called $frac\_secs$. When writing the fractional part to file, in C or C++, by default only 6 decimal places are written. This reduces the timestamp resolution to 1 μs and hence the positioning granularity to 300 m. The effect of this on the timestamps is shown in Figure 4.18:

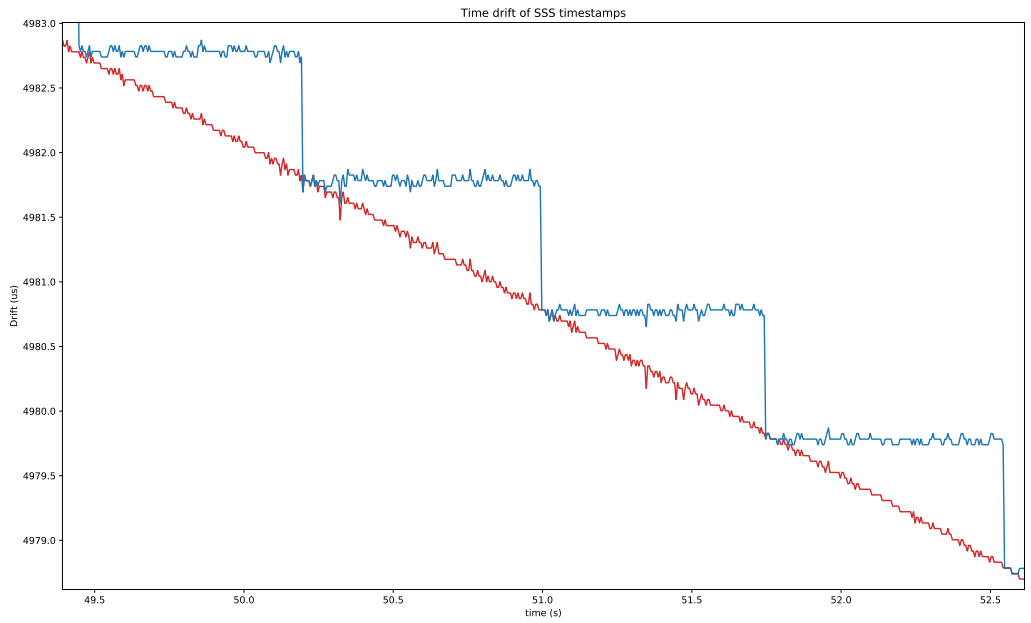


Figure 4.18 The blue graph shows the effect of rounding the SSS timestamps to the nearest microsecond; which causes the time drift of SSS timestamps to appear staircase shaped rather than continuous (red graph) which is what it would look like.

To prevent this the number of decimal places must be explicitly specified as shown:

```
/* Write double with 9 decimal places. */
fprintf(filename, ``%.9f'', full_secs);
```

2. **Getting timestamps from the PC**
   The initial method of obtaining the TOA of SSS sequences was to add a timestamp after the immediate end of the SSS correlation process and then subtract the correlation-process' processing time to obtain its actual TOA. There are various issues with this method, i.e.,:

   (a) The SSS correlation process does not run at hard-scheduled times, i.e., exactly every 5 ms, because Ubuntu Linux is a general-purpose operating system (GPOS), and not deterministic[26] [8]; hence, it is unable to do this.

   (b) In GPOSs, processes can be interrupted, causing them to execute later than scheduled, adding an additional error to the timestamps [8].

   (c) PC functions have large delays because they run at the user-space and not kernel-space[27]; i.e., the C function that obtains a timestamp can take a long time from when it is called to when it obtains the timestamp.

[26] Only Real-Time Operating Systems (RTOS) are deterministic.

[27] To protect the computer, user applications can not directly run on the hardware. User applications communicate with the kernel which then communicates with the hardware. The disadvantage of this is extra overhead.

Another major issue is that timestamps obtained using C functions only have a resolution of 1 μs[‖], providing a positioning granularity of only 300 m, which is insufficient for this project.

Because of the reasons listed, time-stamping the TOA of the SSS sequences using C/C++ functions is unreliable, as made evident by Figure 4.19, which shows the period of SSS TOAs ranging from near 0 to 15,000 μs instead of being at (more or less) exactly 5 ms.

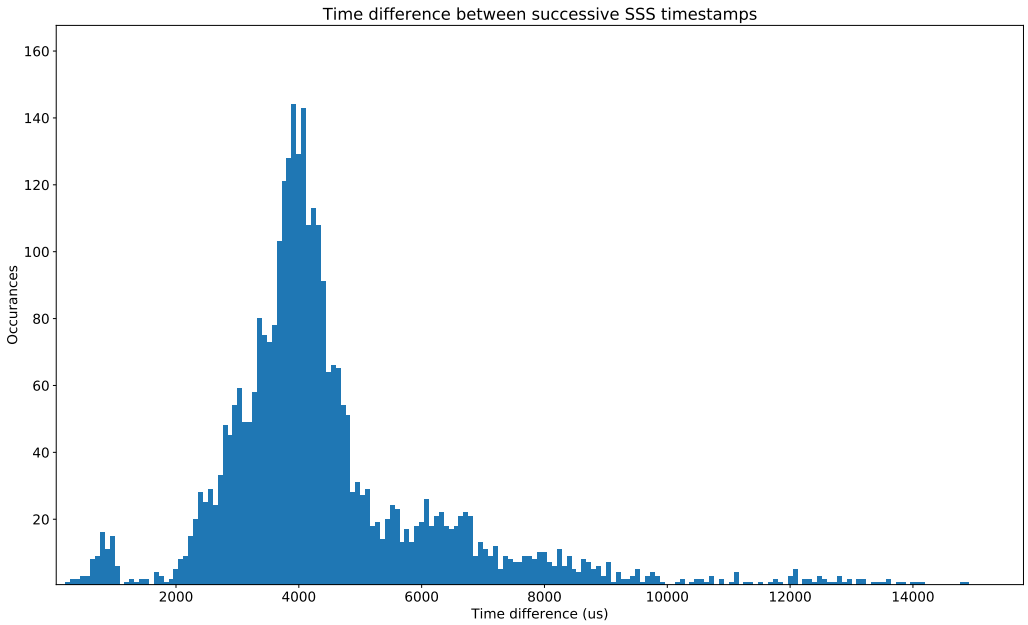


Figure 4.19 Period of SSS TOAs, when the TOAs are timestamped by the PC (i.e., C library functions). Due to the nondeterministic nature of GPOSs, the timestamps are not applied at the right time. Hence, the period of TOAs range from near 0 to around 15,000 μs instead of being (more or less) exactly 5000 μs. Data obtained from a stationary UE.

[‖]See `https://en.cppreference.com/w/cpp/chrono/c/CLOCKS_PER_SEC`

4.12 CONCLUSIONS AND FUTURE WORK

4.12.1 Conclusions and Recommendations

This chapter started by explaining how the TOA of periodic pilot sequences transmitted by the LTE cellular network can be used to for positioning. It stated a theoretical positioning accuracy of 1 sampling period, which at 23.04 MHz is 43.4 ns; equating to a positioning granularity and theoretical accuracy of 13 m.

In order to timestamp the TOA of the pilot sequences a software-defined LTE UE was used — which was made up of a USRP B200mini SDR front-end and srsUE (a software implementation of an LTE UE written in C and C++).

LTE pilot sequences are transmitted periodically every 5 ms. By capturing real LTE signals and analysing their TOA, the TOAs were found to have a shorter period (shorter by ∼5.5 ns) than 5 ms; resulting mainly from the time drift of the low quality UE clock (a TCXO) since the eNB clocks were high precision GPS disciplined OCXOs [42]. The TOAs were detected with an accuracy of 127 ns (1σ) in the presence of multipath (i.e., inside a building), and typically with an accuracy of 65 ns (1σ) with less multipath (i.e., when the UE antennas were mounted on the windscreen of a car facing the eNB). This equates to a practical accuracy of 76 m (2σ) and 39 m (2σ) respectively; assuming the UE's clock drift can be compensated. To improve the system's accuracy, the TOAs can be detected with sub T_s resolution by using the Blais-Rioux algorithm [15] and by removing the effects of multipath; a solution to the latter is provided in [24].

The biggest contributor of errors was the UE clock's time drift. Hence, for a practical and reliable positioning system either a higher quality clock or a robust method of modelling its drift is needed so that it can be compensated. The drift rate of low quality clocks, such as the B200mini's TCXO, was found to be volatile and non-linear. Hence, it will be either difficult or impossible to accurately model. Thus, a higher quality clock, such an OCXO, will likely be a necessity. The drift rate of these clocks are linear over a longer period of time, and should be predictable over a period of ∼1 hour; the typical duration of flight of a fully electric VTOL UAV.

A solution is provided for the situation where no drift compensation method is available. In such a situation both the UE and eNB will need to be equipped with even higher quality clocks. An option for the UE is the CSAC GPSDO [7] from Jackson Labs and for the eNB the IQCM-100 GPS-Disciplined OCXO [34] from IQD. Both clocks have a holdover of less than 2 μs over 24 hours, and hence, should allow the UAV to operate reliably in the absence of GNSS for ∼2 hours without drift compensation.

While the use of a CSAC GPSDO on the UAV is at the discretion of the UAV owner, upgrading the eNB clocks is not. In which case, the UE will need to model and estimate the drift of the eNB clock, although, this may not be possible. Since the eNB OCXOs are continually disciplined by GPS, their drift is constantly corrected.

Hence, it cannot be observed and modeled, meaning no drift compensation. Without drift compensation, an eNB clock's drift, will likely reach an error of 100 m in around 5–10 minutes (based on results from Section 4.8.3), at which point the UAV can no longer rely its LTE based positioning system. Although 5–10 minutes is insufficient for the entire duration of a UAVs flight, it is plenty for emergency landings. Since GNSS availability in developed countries is near a 100 %, this may be satisfactory.

4.12.2 Future Work

In order produce a fully functional and practical positioning system, several additional tasks need to be completed — which are discussed in this section.

The obvious one is that srsLTE will need to be modified to track multiple pilot sequences. This is required in order to obtain multiple pseudoranges so that a unique positioning fix can be obtained. Currently srsUE only tracks pilot sequences from its serving eNB, which can only provide one pseudorange.

Additionally, in order to utilise all available eNBs, srsUE will need to be modified so that it can search the entirety of the LTE bands specified. In New Zealand LTE bands 28 (700 MHz), 3 (1800 MHz), and 7 (2600 MHz) are used. There are three networks, and each network is allocated 20 MHz on each individual band. By being able to search the entirety of a band, the UE will be able to utilise all eNBs on that band. srsLTE provides an example called *cell_search* which can be used to search for networks on a specified band by searching the entire band. Although *cell_search* is not part of srsUE, it should be possible to embedded it in to the srsUE. In practice, operating at multiple frequencies will likely require multiple radio front-ends, each operating at a different frequency, since changing radio frequencies is rather slow.

Another task is to remove all higher level processes since they are only needed for passing information (i.e. data) to the application layer. These layers are not needed for positioning and should be removed to reduce code complexity, size, and clutter.

Finally, srsUE should be modified to track each pilot sequence less frequently in order to reduce computation, e.g,. 20–50 times per second for each SSS rather than the default 100 times per second. The default is 100 because there are 100 frames in a second and each frame contains two unique SSS sequences. Since the UE must know the start of each frame, it must decode (more or less) every single SSS sequences, which is not a requirement for positioning.

Appendix A

CONNECTING LARA-R280 TO M-CENTER

In order to communicate with the LARA-R280, run m-center, select an AT port, and connect using the following port settings [44]:

- Data rate: 115,200 bit/s
- Data bits: 8
- Parity: N
- Stop bits: 1
- Flow control: HW

Appendix B

TIMING ADVANCE SCRIPTS

```
import serial

#=========================================================================
# Functions

def read_rsp():                 # reads a commands response
    msg = ms.readline(); print(msg)

    while b'OK' not in msg:     # keep looping until 'OK' is found.
        if msg == b'':
           break                # o/w the loop will go on forever

        msg = ms.readline(); print(msg);

#=========================================================================
# Define port settings

ms = serial.Serial('COM12',baudrate=115200,timeout=5,rtscts=True,dsrdtr=True)
ms.open()           # open cellular port
ms.dsrdtr = False   # taking the DSR from ON-to-OFF enters command mode

#=========================================================================
# Initialised GNSS and cellular modems

ms.write(b'AT+CMEE=2\r')
ms.write(b'AT+CREG=2\r')      # enable network reg/location info URC
ms.write(b'AT+UGPS=1,1\r')    # turn on GNSS module.
ms.write(b'AT+UGIND=1\r')
ms.write(b'AT+CMGF=1\r')
ms.write(b'AT+CSDH=1\r')
ms.write(b'AT+CGSMS=2\r')
ms.write(b'AT+UGGLL=1\r')

#-------------------------------------------------------------------------
# Setup Packet Switched Data (PSD) connection

```

```
ms.write(b'AT+UPSD=0,0,0\r')
ms.write(b'AT+UPSD=0,1,"wap.telecom.co.nz"\r')
ms.write(b'AT+UPSD=0,4,"8.8.8.8"\r')
ms.write(b'AT+UPSD=0,5,"8.8.4.4"\r')
ms.write(b'AT+UPSD=0,100,8\r')
ms.write(b'AT+UPSDA=0,3\r')
ms.write(b'AT+CGDCONT?\r')
ms.write(b'AT+UPING="www.google.com"\r')
ms.write(b'AT+UPSND=0,0\r')
ms.write(b'AT+UPSND=0,8\r')
ms.write(b'AT+CGATT?\r')
ms.write(b'AT+CGACT?\r')
ms.write(b'CGPADDR=1,8\r')
ms.write(b'AT+CGREG=2\r')
ms.write(b'AT+UREG=1\r')
ms.write(b'AT+CGCONTRDP=1\r')
ms.write(b'AT+CGCONTRDP=8\r')

#=========================================================================
# Get TA value and GPS fix

i = 0
while (True):
    print('\niteration:'+str(i))

    ms.write(b'AT+UPING="www.google.com"\r'); read_rsp()

    ms.reset_output_buffer()
    ms.write(b'AT+CGED=0,0\r'); read_rsp()

    ms.reset_output_buffer()
    ms.write(b'AT+UGGLL?\r'); read_rsp()

    i += 1
```

Appendix C

COST OF VOR AND DME SYSTEM

DME Antenna
1/4 wave shark fin.

VOR/LOC Antenna
V-type Dipole.

Co-axial cable

Co-axial cable

VOR Receiver (NAV/COMM). Displays VOR and COMM channel frequencies as well as handling frequency channeling for VOR, DME, and COMM.

DME channelling signal

E.g., 2x5 ARINC parallel data bus.

DME Interrogator

VOR RX output data bus.

DME output data bus.

DME Indicator. Displays distance to ground beacon in NM, ground speed in knots, and time to station (TTS) in minutes.

VOR Indicator. Displays bearing and whether the aircraft is moving towards or away from the beacon. This is indicated by the TO and FR indicators respectively.

Cost of system (assuming brand new components)

Item	Cost (low end)	Cost (high end)
VOR antenna	$230	$1,600
DME antenna	$164	$433
DME interrogator	$10,000	$34,000
VOR receiver	$3,000	$6,400
DME display	$3,400	$5,800
VOR indicator	$2,250	$3,300
Total	**$19,044**	**$51,533**

REFERENCES

[1] 2001 federal radionavigation systems. Technical report, Department of Defense and Department of Transportation, 2001.

[2] Radio subsystem synchronization. Technical Specification 05.10, 2003. URL https://www.3gpp.org/ftp/Specs/archive/05_series/05.10/.

[3] *Instrument Flying Handbook*. U.S. Department of Transportation, Federal Aviation Administration, 2012.

[4] Evolved universal terrestrial radio access (e-utra); physical channels and modulation. Technical Specification 36.211, 3GPP, 2016. URL https://www.3gpp.org/ftp/Specs/archive/36_series/36.211/.

[5] New zealand ground based navigation aid infrastructure strategy. Technical report, New Southern Sky, November 2016. URL https://www.nss.govt.nz/dmsdocument/27-ground-based-navigation-aid-strategy.

[6] Gpsdo kit for usrp n200/n210, April 2019. URL https://www.ettus.com/all-products/gpsdo-kit/.

[7] Chip scale atomic clock gpsdo, April 2019. URL http://www.jackson-labs.com/index.php/products/csac.

[8] What is a real-time operating system (rtos)? White paper, National Instruments, March 2019. URL http://www.ni.com/en-us/innovations/white-papers/07/what-is-a-real-time-operating-system--rtos--.html.

[9] 3GPP. 3gpp ts 36.321 v15.1.0. Technical report, 3GPP, 03 2018.

[10] aircraftspruce.com. Comant vor/loc/gs (ci-120-400), 2017. URL http://www.aircraftspruce.com/pages/av/antenna_vornav/comant120400.php.

[11] W. Anderson. The accuracy of the vhf omni-range system of aircraft navigation; a statistical study. *IRE Transactions on Aeronautical and Navigational Electronics*, (1):25–37, 1955.

[12] C. A. S. A. Australia. Operational notes on distance measuring equipment. 2005.

[13] C. A. S. A. Australia. Operational notes on non-directional beacons (ndb) and associated automatic direction finding (adf). 2005.

[14] C. A. S. A. Australia. Operational notes on vhf omni range (vor). 2005.

[15] F. Blais and M. Rioux. Real-time numerical peak detector. *Signal Processing*, 11 (2):145–155, 1986.

[16] R. S. Campos. Evolution of positioning techniques in cellular networks, from 2g to 4g. *Wireless Communications and Mobile Computing*, 2017, 2017.

[17] J. Cartright. *Choosing an AT or SC cut for OCXOs*. Connor-Winfield Corporation, 10 2008.

[18] H. D. Curtis. *Aerospace Engineering Desk Reference*. Butterworth Heinemann, 2009.

[19] E. Dahlman, S. Parkvall, and J. Skold. *4G LTE / LTE-Advanced for Mobile Broadband*. Academic Press, 2011.

[20] M. Driusso, C. Marshall, M. Sabathy, and et al. Vehicular position tracking using lte signals. *IEEE Transactions on Vehicular Technology*, 66(4):3376–3391, 2017.

[21] Ericsson. Positioning with lte. 2011.

[22] A. Faria. Dme âĂŞ distance measuring equipment, 2011. URL `https://leagueofextraordinarytechnicians.wikispaces.com/DIstance+Measuring+Equipment++-+Operation`.

[23] W. I. Forum. What is software defined radio, April 2019. URL `https://www.wirelessinnovation.org/assets/documents/SoftwareDefinedRadio.pdf`.

[24] Z. Kassas, J. Khalife, K. Shamaei, and et al. Computationally efficient receiver design for mitigating multipath for positioning with lte signals. 2017.

[25] Z. Kassas, J. Khalife, K. Shamaei, and et al. I hear, therefore i know where i am: Compensating for gnss limitations with cellular signals. *IEEE signal processing magazine*, 34(5):111–124, 2017.

[26] M. Kovaleva. Global 2g phase out: What do we know so far?, 2018. URL `https://www.emnify.com/blog/global-2g-phase-out`.

[27] S. Labs. Recommended crystal, tcxo, and ocxo reference manual for high-performance jitter attenuators and clock generators, April 2019. URL `https://www.silabs.com/documents/public/reference-manuals/si534x-8x-9x-recommended-crystals-rm.pdf`.

[28] T. Layh, J. Larson, D. Gebre-Egziabher, B. Taylor, J. Jackson, and Y. Agamawi. Gps-denied navigator for small uavs. Final report, University of Minnesota UAV Laboratory, Department of Aerospace Engineering Mechanics, 2014.

[29] K. Maier and J. Demel. Gnu radio lte receiver, 2014. URL `https://github.com/kit-cel/gr-lte`.

[30] P. Marzioli, A. Pellegrino, M. Valdatta, F. Curianò, F. Angeletti, L. Frezza, A. Gianfermo, L. Arena, T. Cardona, F. Piergentili, et al. Testing the vor (vhf omnidirectional range) in the stratosphere: Stratonav experiment. In *Metrology for Aerospace (MetroAeroSpace), 2016 IEEE*, pages 336–341. IEEE, 2016.

[31] MathWorks. Synchronization signals (pss and sss). URL https://www.mathworks.com/help/lte/ug/synchronization-signals-pss-and-sss.html.

[32] J. Ostermeier. Test of dme/tacan transponders - application note. Technical report, Rhode Schwarz, 2009.

[33] K. S. Pasupuleti. Timing advance and time alignment timer, 2014. URL http://howltestuffworks.blogspot.com/2014/07/timing-advance-and-time-alignment-timer.html.

[34] I. F. Products. Ocxo specification iqcm-100, April 2019. URL https://www.iqdfrequencyproducts.com/products/details/iqcm-100-2-34.pdf.

[35] E. Research. Usrp hardware driver and usrp manual, 2019. URL https://files.ettus.com/manual/index.html.

[36] A. Schmidt-Dannert. Positioning technologies and mechanisms for mobile devices.

[37] K. Shamaei, J. Khalife, and Z. Kassas. Performance characterisation of positioning in lte systems. 2016.

[38] B. Singh. Analysis of cellular positioning techniques in umts networks. 2014.

[39] Spirent. An overview of lte positioning. 2012.

[40] S. R. Systems. Open source sdr lte software suite, 2018. URL https://github.com/srsLTE/srsLTE.

[41] P. Tom Rogers. Adf basics, 1998. URL https://www.avweb.com/news/avionics/183233-1.html.

[42] G. Tunnicliffe. How is network synchronization achieved in lte? Personal Correspondence, June 2018.

[43] T. N. Tye. Application of digital signal processing methods to very high frequency omnidirectional range (vor) signals in the design of an airborne flight measurement system. Masters thesis, Russ College of Engineering and Technology, Ohio University, 1996.

[44] U-blox. *TOBY-R2 and LARA-R2 series Cellular Evaluation Kits User Guide*, 12 2017.

[45] U-blox. *LARA-R2 series: Size-optimized LTE Cat 1 modules in single and multi-mode configuration: Data Sheet*, 12 2017.

[46] *Aeronautical Information Manual - Official Guide to Basic Flight Information and ATC Procedures*. U.S. Department of Transportation, Federal Aviation Administration, 2017.

[47] Wikipedia. Internet in new zealand. URL https://en.wikipedia.org/wiki/Internet_in_New_Zealand.

[48] Wikipedia.org. Distance measuring equipment, 2017. URL https://en.wikipedia.org/wiki/Distance_measuring_equipment.

[49] B. Wojtowicz. Openlte, 2017. URL http://openlte.sourceforge.net/.